Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Profesional de Ingeniería de Sistemas

Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación

TESIS

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Carolina Rubí CÁCEDA RODRÍGUEZ

ASESOR

Mg. Marcos Hernán RIVAS PEÑA

Lima, Perú

2021

Referencia bibliográfica

Cáceda, C. (2021). *Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación*. Tesis para optar el título de Ingeniero de Sistemas. Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas, Universidad Nacional Mayor de San Marcos, Lima, Perú.

HOJA DE METADATOS COMPLEMENTARIOS

Código ORCID del autor	—
DNI o pasaporte del autor	48022736
Código ORCID del asesor	0000-0002-5138-381X
DNI o pasaporte del asesor	09241816
Grupo de investigación	NO
Agencia financiadora	NO
Ubicación geográfica donde se desarrolló la investigación	Lima, Perú.
Año o años que abarcó la investigación	2018 al 2019
Disciplinas OCDE	**Ingeniería de sistemas y comunicaciones** https://purl.org/pe-repo/ocde/ford#2.02.04

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación de Tesis

Siendo las 3pm horas del día 28 de enero del año 2021 se reunieron virtualmente los docentes designados como miembros de Jurado de Tesis, presidido por el Dr. Javier Gamboa Cruzado(Presidente), el Dr. Frank Escobedo Bailón(Miembro) y el Mg. Marcos H. Rivas Peña(Miembro Asesor), usando la plataforma Meet para la sustentación Virtual de la tesis Intitulada: **"Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación",** de la Bachiller: **Carolina Rubí Cáceda Rodríguez;** para obtener el Título Profesional de Ingeniero de Sistemas.

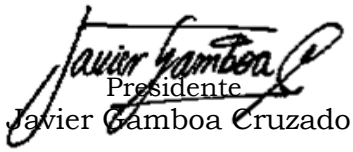
Acto seguido de la exposición de la Tesis, el Presidente invitó a la Bachiller a dar las respuestas a las preguntas establecidas por los Miembros del Jurado.

La Bachiller, en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, la bachiller obtuvo la nota de 18 (dieciocho).

A continuación el Presidente del Jurado Dr. Javier Gamboa Cruzado, declara a la Bachiller **Ingeniero de Sistemas.**

Siendo las 4 pm horas, se levantó la sesión.



Presidente
Dr. Javier Gamboa Cruzado

Miembro
Dr. Frank Escobedo Bailón

Miembro Asesor
Mg. Marcos Rivas Peña

FICHA CATALOGRÁFICA

CÁCEDA RODRÍGUEZ, Carolina Rubí

MODELO DINÁMICO PARA LA GESTIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Línea de Investigación: Plataforma TIC, Cyber Seguridad
Lima, Perú. 2021

Tesis, Facultad de Ingeniería de Sistemas, Escuela Profesional Ingeniería de Sistemas, Pregrado, Universidad Nacional Mayor de San Marcos.

Formato 28 x 20 cm Páginas 123

AGRADECIMIENTOS

Al profesor Rivas Peña, Marcos Hernán (UNMSM) por su apoyo permanente, dedicación que demostró desde un inicio y aporte importante a la presente tesis.

Al profesor Lomparte Alvarado, Rómulo Fernando (ISACA) por la retroalimentación realizada, la validación del modelo y el apoyo recibido a la presente tesis.

Al Ingeniero Alva Lizarraga, Alfredo (Banco de Comercio) por compartir sus conocimientos y experiencias como guía a la presente tesis.

Al profesor Ugáz Cachay, Winston (UNMSM) por compartir sus conocimientos para el desarrollo del modelo.

A los miembros del jurado por su evaluación crítica.

A todas aquellas personas que aportaron conocimientos, gracias, al profesor Cámara Figueroa, Adegundo Mario (UNMSM), a la profesora Castro León, Gloria Helena (UNMSM) y al Ingeniero Castro Mayorca, Diego Alonso (Tata Consultancy Services).

A Dios por ser mi guía constante.

A todos, ¡muchas gracias!

Dedicatoria

A mi madre Olga, principal fortaleza para seguir adelante y a mi abuelito Santiago, mi inspiración.

ÍNDICE GENERAL

CAPÍTULO 3: ESTADO DEL ARTE

Lista de tablas

Lista de figuras

MODELO DINÁMICO PARA LA GESTIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Autor: CÁCEDA RODRÍGUEZ, Carolina Rubí

Asesor: RIVAS PEÑA, Marcos Hernán

Título: Tesis para optar el Título de Ingeniero de Sistemas

Fecha: Enero de 2021

Resumen

Actualmente las vulnerabilidades de las infraestructuras tecnológicas críticas generan una gran preocupación nacional en seguridad, los ciber-riesgos se consolidan en el panorama de riesgos globales. Por otro lado, los ataques cibernéticos cada año crecen ocasionando que la ciberseguridad se convierta en uno de los riegos más críticos del mundo.

En base a estos antecedentes se propone desarrollar un modelo dinámico como herramienta de gestión, basado en las técnicas de dinámica de sistemas con la finalidad de mejorar la toma de decisiones estratégicas en seguridad de las organizaciones.

Este modelo permite gestionar las vulnerabilidades y prevenir ataques bajo diversos escenarios, determinando a través de indicadores de alertas, ataques y vulnerabilidades, si la aplicación del modelo favorece los procesos y protección de los activos de las TIC.

Palabras clave: seguridad de la información, seguridad informática, ciberseguridad, dinámica de sistemas, modelo dinámico, TIC, infraestructura de las TIC.

DYNAMIC MODEL FOR INFRASTRUCTURE SECURITY MANAGEMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Author: CÁCEDA RODRÍGUEZ, Carolina Rubí

Adviser: RIVAS PEÑA, Marcos Hernán

Title: Thesis to choose the Professional Title System Engineer

Date: January 2021

Abstract

Currently, the vulnerabilities of critical technological infrastructures generate a great national concern in security, cyber risks are consolidated in the global risk landscape together. On the other hand, cyber-attacks every year grow causing cybersecurity to become one of the most critical risks in the world.

Based on this background, it is proposed to develop a dynamic model as a management tool for decision making, based on systems dynamics techniques in order to improve strategic decision making in organizations security.

This model allows manage vulnerabilities and prevent attacks under various scenarios, determining through indicators of alerts, attacks and vulnerabilities, if the application of the model favors the processes and protection of ICT assets.

Key words: information security, computer security, cybersecurity, system dynamics, dynamic model, ICT, ICT infrastructure.

CAPÍTULO 1: INTRODUCCIÓN

1.1 Antecedentes

La propuesta de Pastor (2010), en su tesis "Impacto del riesgo en el Gobierno de las Tecnologías de Información y Comunicación en la Gestión Empresarial Industrial del Siglo XXI", evalúa en qué medida la implementación de un sistema de gestión del riesgo contribuye en la creación de ventajas competitivas basado en el gobierno de Tecnología de Información y Comunicación (TIC), optimización de procesos y conocimientos obtenidos a partir de la experiencia. Según el autor la implementación de un planteamiento estratégico en Tecnología de Información (TI) favorece el desarrollo de la optimización de procesos.

En junio del 2012 Information Systems Audit and Control Association (ISACA), publica la guía "Control Objectives for Information and Related Technology (COBIT5) para la Seguridad de la Información" con la finalidad de ayudar a los profesionales de TI y seguridad, a tomar decisiones más informadas en seguridad de la información.

Por su parte Nazareth & Choi (2015), proponen un modelo de dinámica de sistemas para la gestión de la seguridad de información, donde enfatizan la necesidad de adoptar una cartera de estrategias en lugar de una solución. A través del modelo se llegó a una mejor rentabilidad en las inversiones de herramientas de seguridad para la detección de ataques. Según los autores es necesario invertir en todas las áreas de seguridad para proteger eficazmente la información.

A pesar de esto según ISACA (2015) el 83 % de los ataques cibernéticos, son uno de los tres problemas más latentes en los negocios, pero solo el 38% se siente preparado para un ataque informático, a su vez Cisco en su reporte anual de la seguridad menciona que, de sus 115 000 dispositivos en internet analizados, el 92% de ellos ejecutaba software con vulnerabilidades conocidas. Además, el 31% de sus dispositivos en uso que se incluyeron en el análisis ya no se comercializa y el 8% ya ha alcanzado el fin de su ciclo de vida útil. (Cisco, 2016, pp. 35-36)

Otra investigación importante es la de Khalil (2016) que establece un modelo dinámico para simular ataques, utilizando la técnica de Montecarlo, el modelo lo aplicó en una planta de procesos químicos, resultando un 64.4 % de probabilidad de éxito en la misión de ataque. El modelo ayudó a incrementar estrategias defensivas.

Mai, Parsons, Prybutok, & Namuduri (2017), publican un artículo sobre un nuevo enfoque del modelo conceptual para la seguridad de la información basados en la ciencia cognitiva y la neurociencia, donde desarrollan experimentos con procesos automáticos que mejoran los procesos de toma de decisiones.

Okoye (2017) en un estudio de doctorado propone diez estrategias para reducir los efectos de las amenazas de seguridad en opinión de líderes empresariales de Nigeria, se concluye que los líderes de las pymes necesitan un sistema de estrategias efectivas y habilidades de liderazgo para minimizar los efectos de las amenazas.

Los modelos dinámicos contribuyen en diferentes aspectos para la evaluación de estrategias, Mendoza (2018) en su tesis "Modelo de Dinámica de Sistemas para la evaluación de estrategias de fidelización al cliente" propone un modelo basado en la metodología de dinámica de sistemas con la finalidad de elegir la mejor estrategia para la fidelización del cliente logrando reducir significativamente el tiempo de evaluación de estrategias en fidelización y ayudando a los directivos a tomar la mejor decisión.

Por otro lado, el Foro Económico Mundial (WEF), en enero de 2018 crea el nuevo Centro Global de Ciberseguridad que ofrece la primera plataforma para gobiernos, empresas y organizaciones internacionales para disminuir el impacto de las actividades maliciosas en la web, reconociendo a la ciberseguridad como uno de los riesgos más críticos del mundo. (WEF, 2018)

Huawei (2018) ha desarrollado HiSec, una solución que provee a sus clientes seguridad de infraestructura inteligente de TIC, su arquitectura de seguridad definida por software posee tres capas: la primera es el ejecutor, responsable del manejo de amenazas y recopilación de información; la segunda que es el controlador, que administra la forma de cooperación de ejecutor y recibe las instrucciones de una tercera capa que es el analizador, esta recopila información de las amenazas, basada en el aprendizaje automático.

Sin embargo, las vulnerabilidades de las infraestructuras tecnológicas críticas son una gran preocupación nacional en seguridad, los ciber-riesgos se consolidan en el panorama de riesgos globales junto a la posición de los riesgos ambientales en el cuadrante de alto impacto y alta probabilidad, estos conducen al robo de dinero y datos (82%) e interrupción de operaciones (80%).

(WEF, 2019, p. 16). En la actualidad los problemas de seguridad de Tecnologías de Información (TI) y privacidad, junto con la ciberseguridad, se clasifican como el principal desafío tecnológico. (ISACA, Protiviti, 2019). Por ello resulta necesario un enfoque dinámico para esta problemática de la gestión de seguridad de la infraestructura de las TIC.

1.2 Definición del problema

Las organizaciones no cuentan con un modelo definido para la gestión de seguridad de la infraestructura de las TIC, esto conlleva a la presencia de un alto nivel de riesgo en los procesos, las funciones que realizan los trabajadores en las organizaciones y como resultado una baja calidad, altos costos de mantenimiento de sus activos de información, enfrentar ataques y robos de información, dando lugar a daños en la imagen corporativa, pérdida de credibilidad, clientes, entre otros.

1.2.1 Problema general

¿De qué manera el uso de un modelo dinámico mejorará la gestión de seguridad de la infraestructura de las TIC?

1.2.2 Problemas específicos

- PE1: ¿De qué manera el uso de un modelo dinámico disminuirá el número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC?
- PE2: ¿De qué manera el uso de un modelo dinámico disminuirá el número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC?

- PE3: ¿De qué manera el uso de un modelo dinámico disminuirá el número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC?

1.3 Objetivos

1.3.1 Objetivo general

Usar un modelo dinámico para mejorar la gestión la seguridad de la infraestructura de las TIC.

1.3.2 Objetivos específicos

- OE1: Disminuir el número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.
- OE2: Disminuir el número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.
- OE3: Disminuir el número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.

1.4 Justificación

La contribución de la presente tesis radica en permitir tomar decisiones con anticipación para proteger activos de información, dotando de valor agregado con estrategias preventivas,

beneficiando a los gerentes y encargados del área de seguridad de la información de la organización.

ISACA (2016) en su reporte sobre el estado de la ciberseguridad predice que la inteligencia artificial aumentará el riesgo a corto plazo 42% y largo plazo 62 %, internet de las cosas expandirá las superficies de ataque y exacerbará el riesgo cibernético.

Según encuesta de Protiviti, ISACA (2017), la ciberseguridad y la gestión de la infraestructura se clasifican como los principales desafíos tecnológicos.

En el informe anual de Cisco menciona que "De acuerdo con una investigación de Cisco que incluyó 130 organizaciones de mercados verticales, el 75 % de dichas empresas sufren infecciones por adware. Los adversarios pueden llegar a utilizar estas infecciones para facilitar otros ataques de malware" … "las organizaciones que aún no han sufrido una infracción a la seguridad pueden creer que sus redes son seguras. Probablemente esta confianza sea inadecuada, si se tiene en cuenta que el 49 % de los profesionales de seguridad encuestados indicaron que sus organizaciones han tenido que enfrentarse al escrutinio público tras una infracción a la seguridad." (Cisco, 2017, p. 5)

Cisco (2017) afirma que un 38% del personal de seguridad de TI experimentó pérdida de ingresos mayor al 20%, como resultado de un ataque, que se presenta en la Figura 1. Por ello es importante usar estrategias preventivas ante un ataque.

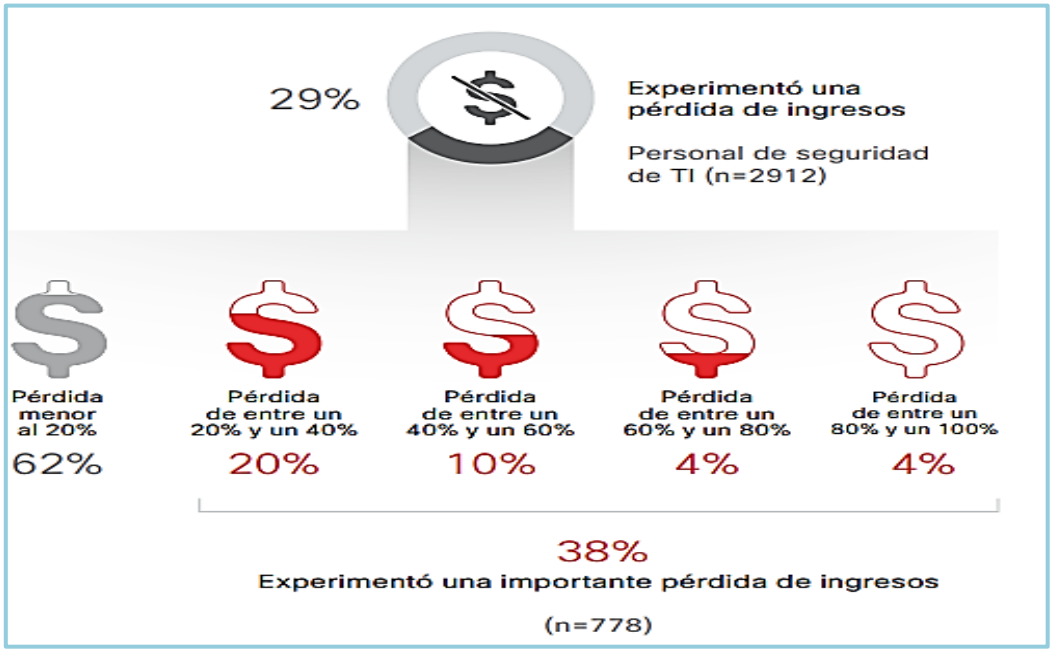


Figura 1. Porcentaje de ingresos de la organización perdidos como resultado de un ataque.

Fuente. Adaptado del Informe anual sobre ciberseguridad. (Cisco, 2017)

En la Figura 2 se puede evidenciar que un 42% de los encargados de seguridad de TI experimentaron pérdidas importantes de oportunidades como resultado de ataques.

Figura 2. Porcentaje de oportunidades empresariales perdidas como resultado de un ataque.

Fuente. Adaptado del Informe anual sobre ciberseguridad. (Cisco, 2017)

Los ataques traen como consecuencia importantes pérdidas de clientes, que se presenta en la Figura 3.

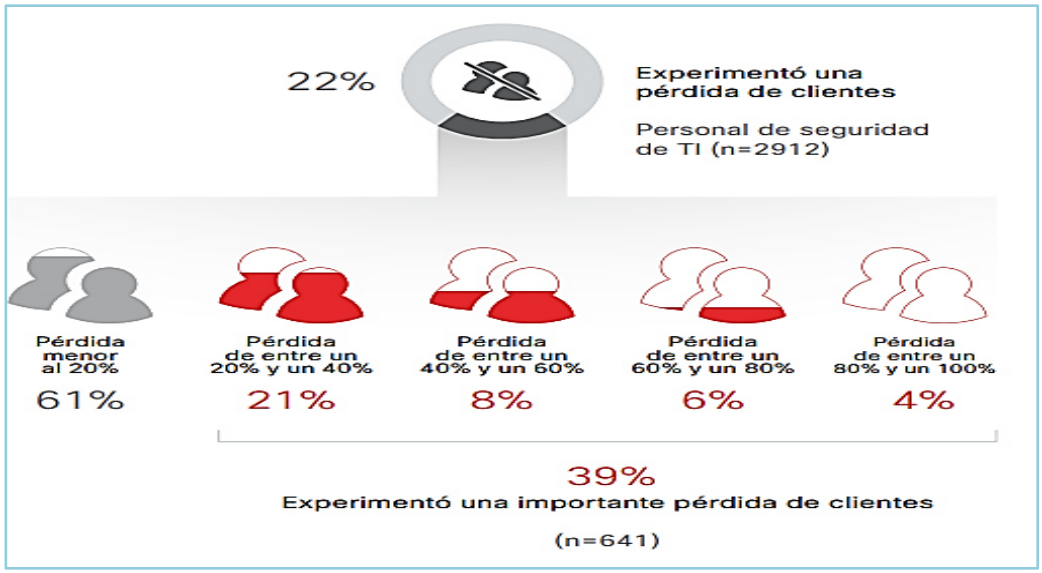


Figura 3. Porcentaje de clientes perdidos por las empresas como resultado de un ataque.

Fuente. Adaptado del Informe anual sobre ciberseguridad. (Cisco, 2017)

Cisco (2017), en su Reporte Semestral de Seguridad, afirma que "En las empresas de todos los tamaños, un enfoque más holístico en la seguridad ofrecerá una protección más eficiente contras las amenazas en evolución. … una vista holística de las amenazas… es deseable para tener una real efectividad de la seguridad informática." (pp. 62-63)

En la Figura 4 se puede evidenciar que las simulaciones contribuyen mejorar sustancialmente los niveles de seguridad, en políticas y procedimientos, en opinión de profesionales especializados en seguridad.

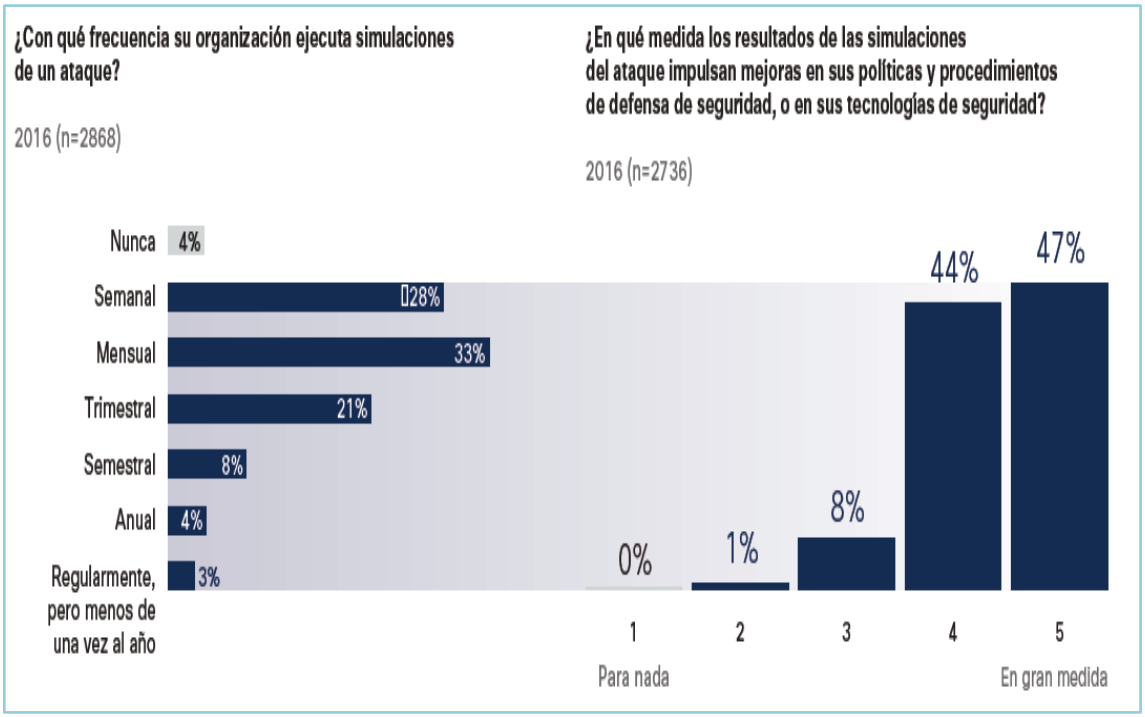


Figura 4. Simulación de ataques: frecuencia y alcance de implementar mejoras en la defensa de la seguridad.

Fuente. Adaptado del Informe anual sobre ciberseguridad. (Cisco, 2017)

1.5 Alcances

El presente modelo se limita a simular escenarios de seguridad que permita tomar decisiones para la protección de la infraestructura de TIC en las organizaciones, para ello se requieren parámetros que pueden ser adaptados y calibrados en diferentes escenarios, aplicando dinámica de sistemas, sustentado sobre publicaciones y la opinión de expertos, que permitan minimizar riesgos ante las diferentes amenazas, dotando de valor agregado a la gestión de seguridad de la infraestructura de las TIC.

La prueba y aplicación de la tesis es en un banco del sector financiero, sin embargo, se puede aplicar a cualquier sector, las variables son sobre seguridad de la información y no son exclusivas de un sector.

1.6 Hipótesis

1.6.1 Hipótesis general

Si se usa un modelo dinámico, entonces mejora la gestión de seguridad de la infraestructura de las TIC.

1.6.2 Hipótesis específicas

- HE1: Si se usa un modelo dinámico, entonces disminuye el número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.
- HE2: Si se usa un modelo dinámico, entonces disminuye el número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.
- HE3: Si se usa un modelo dinámico, entonces disminuye el número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.

1.7 Variables e indicadores

Variables:

- **Variable Independiente:** Modelo dinámico.
- **Variable Dependiente:** Gestión de seguridad de la infraestructura de las TIC.

Indicadores:

- **Conceptualización**

  Variable Independiente: Modelo dinámico.

  En la Tabla 1 se describe el indicador para el modelo dinámico.

  Tabla 1. Descripción del indicador de la variable independiente.

Indicador	Descripción
Presencia - ausencia.	Cuando es no, es porque no existe un modelo dinámico que contribuye con la gestión de la seguridad de la infraestructura de las TIC. Cuando es si, es porque existe un modelo dinámico que contribuye con la gestión de la seguridad de la infraestructura de las TIC.

  Variable Dependiente: Gestión de seguridad de la infraestructura de las TIC.

  En la Tabla 2 se describe los indicadores para la Gestión de seguridad de la infraestructura de las TIC.

Tabla 2. Descripción de los **i**ndicadores de la variable dependiente.

Indicador	Descripción
Número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.	Cantidad de alertas registradas por inadecuada definición o configuración de accesos a la infraestructura de las TIC.
Número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.	Cantidad de ataques por ausencia de implementación de medidas de seguridad informática que afectaron la infraestructura de las TIC.
Número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.	Cantidad de vulnerabilidades encontradas en el diseño, implementación o control interno de proceso que puede exponer al sistema a amenazas.

- **Operacionalización**

Variable Independiente: Modelo dinámico.

En la Tabla 3 se puede identificar el índice para el modelo dinámico.

Tabla 3. Medición del indicador de la variable independiente.

Indicador	Índice
Presencia - ausencia.	No, Sí.

Variable Dependiente: Gestión de seguridad de la infraestructura de las TIC.

En la Tabla 4 se detalla la medición y unidad de medida para cada uno de los indicadores de la gestión de seguridad de la infraestructura de las TIC.

Tabla 4. Medición del indicador de la variable dependiente.

Indicador	Índice	Unidad de medida
Número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.	<500- > No aceptable. <100-500] De cuidado. [0-100] Aceptable.	**# de alertas/mes**
Número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.	<6- > No aceptable. <3-6] De cuidado. [0-3] Aceptable.	**# de ataques/mes**
Número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.	<600- > No aceptable. <300-600] De cuidado. [0-300] Aceptable.	**# de vulnerabilidades/mes**

1.8 Organización de la tesis

La presente tesis se encuentra organizada en seis capítulos, los cuales se describen a continuación.

En el Capítulo dos se detalla el marco teórico de la tesis, que involucra la gestión de seguridad, las TIC, infraestructura de las TIC, amenazas, vulnerabilidades, alertas, ataques, COBIT, Business Model for Information Security (BMIS), modelo dinámico, pensamiento

sistémico y la dinámica de sistemas, que son conceptos necesarios para comprender un modelo de gestión de seguridad de infraestructura de las TIC.

En el Capítulo tres se presenta el estado del arte, se describe los diferentes trabajos relacionados a la dinámica de sistemas para afrontar temas de seguridad y una comparación del porqué se utiliza esta metodología.

En el Capítulo cuatro se describe el desarrollo del modelo propuesto que trata acerca del análisis de la solución, la problemática que enfrenta la gestión de seguridad de infraestructura de las TIC y el modelo propuesto que detalla las variables identificadas, el modelo causal y el modelo dinámico, además se presenta escenarios para validar la aplicación del modelo.

En el capítulo cinco se detalla los resultados obtenidos con el modelo y se realiza la contratación de las hipótesis mediante la t de Student.

Finalmente, en el Capítulo seis se presentan las conclusiones y los trabajos futuros para la presente tesis.

CAPÍTULO 2: MARCO TEÓRICO

La primera parte del capítulo explica puntos generales acerca de la gestión de seguridad en la infraestructura de las TIC.

La segunda parte menciona las definiciones de amenazas, vulnerabilidades, alertas, ataques, conceptos que se utilizará en el modelo.

La tercera parte define los aspectos del marco de trabajo COBIT 5, una mención al COBIT 2019 y el modelo de negocio para la seguridad de información.

La última parte trata acerca de los modelos dinámicos, el pensamiento sistémico y la dinámica de sistemas que resultan importantes para el desarrollo del modelo dinámico.

2.1 Gestión de seguridad en la infraestructura de las TIC

Para comprender mejor este concepto se va a desglosar en tres partes: gestión de la seguridad, las TIC y la infraestructura de las TIC.

2.1.1 Gestión de la seguridad

ISACA (2015) en su glosario de términos lo define como "The process of establishing and maintaining security for a computer or network system. Scope Note: The stages of the process of security management include prevention of security problems, detection of intrusions, and investigation of intrusions and resolution." [El proceso de establecer y mantener la seguridad de una computadora o sistema de red. Nota de alcance: Las etapas del proceso de la gestión de seguridad incluye la prevención de problemas de seguridad, detección de intrusiones e investigación de intrusiones y resolución.] (p. 60)

2.1.2 Tecnologías de información y comunicación

El Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC) define a las TIC como "un conjunto de servicios telemáticos, redes, software y dispositivos de hardware que se integran en sistemas de información interconectados y complementarios, con la finalidad de gestionar datos, información y procesos". (CONCYTEC, 2016, p. 8)

Actualmente en el Perú Concytec viene impulsando el Programa Nacional Transversal en Tecnologías de la Información y Comunicación denominado como Evolución de las TIC (E-TIC), que se ejecutará en un horizonte de seis años (2016-2021), con el objetivo de "Generar conocimiento de frontera y desarrollar productos y servicios comercializables en TIC basados en conceptos patentados" (CONCYTEC, 2016, p. 35). Entre el 2011 y el 2015, las publicaciones referentes a las TIC fueron disminuyendo. (CONCYTEC, 2016, p. 18)

2.1.3 Infraestructura de las TIC

La literatura permitió determinar varias definiciones sobre de infraestructura de las TIC.

Gendron (2012) toma la infraestructura de las TIC desde un enfoque de respaldo a la estrategia empresarial.

Huawei (2018) lo describe mediante tres componentes claves:
"computing and processing capacity, connection network, and connected devices." [la capacidad informática y de procesamiento, conexión de red y dispositivos conectados.] (p. 8)

ISACA (2015), define infraestructura de TI como "The set of hardware, software and facilities that integrates an enterprise's IT assets" [El conjunto de hardware, software e instalaciones que integran los activos de TI de una empresa] (p. 39), otro concepto relacionado es el de infraestructura crítica que son "Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation."[Sistemas cuya

incapacidad o la destrucción tendría un efecto debilitante en la seguridad económica de una empresa, comunidad o nación.] (p. 20)

2.2 Términos importantes en el modelo

2.2.1 Vulnerabilidad

Debilidad de un activo o control que puede ser aprovechada por una amenaza. (ISO/IEC 27000, 2009)

2.2.2 Ataque

Intento de destruir, exponer, alterar, inhabilitar, robar u obtener un acceso no autorizado para usar un activo de manera no autorizada. (ISO/IEC 27000, 2009)

2.2.3 Política

Intención general y dirección expresada formalmente por la gerencia. (ISO/IEC 27000, 2009)

2.2.4 Control

El medio de la gestión de riesgos, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o de carácter jurídico. También se utiliza como sinónimo de salvaguardia o de contramedida. (ISO/IEC 27000, 2009)

2.2.5 Dimensión de capacidad

Proporciona una medida de la capacidad de un proceso para satisfacer el negocio actual o proyectado de una empresa, para cumplir con los objetivos del proceso. (ISACA, 2013)

2.2.6 Nivel de capacidad

El nivel de capacidad de un proceso se determina sobre la base del logro de atributos. (ISACA, 2013)

Según Process Assessment Model (PAM) considera los siguientes niveles de capacidad:

- (Nivel 0) Proceso incompleto: Proceso no implementado o no alcanza su propósito.
- (Nivel 1) Proceso ejecutado: Proceso implementado alcanza su propósito.
- (Nivel 2) Proceso gestionado: Proceso implementado de forma gestionada.
- (Nivel 3) Proceso establecido: Proceso gestionado y alcanza sus resultados.
- (Nivel 4) Proceso predecible: Proceso establecido y ejecutado dentro de límites definidos para alcanzar sus resultados.
- (Nivel 5) Proceso optimizado: Proceso predecible y mejorado de forma continua para cumplir con los metas empresariales presentes y futuros.

2.2.7 Exploits

Secuencia de comandos utilizados para aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de exploit se suele perseguir: (Incibe, 2017)

- El acceso a un sistema de forma ilegítima.
- Obtención de permisos de administración en un sistema ya accedido.
- Un ataque de denegación de servicio a un sistema.

2.2.8 Alertas de seguridad

Notificaciones técnicas breves, generalmente legibles por humanos, sobre vulnerabilidades, exploits y otros problemas de seguridad actuales. (NIST, 2016)

2.2.9 Seguridad de la información

La seguridad de la información consiste en la protección de la información independiente de su formato.

"Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)." ISACA (2015) [Asegura que, dentro de la empresa, la información se encuentre protegida contra la divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y no acceso cuando sea necesario (disponibilidad).] (p. 35)

2.2.10 Ciberseguridad

Encargada de la protección de activos digitales, forma parte de la seguridad de información, abarca: "The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems." [La protección de activos de información considerando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados.] (ISACA, 2015, p. 20)

2.2.11 Amenazas persistentes avanzadas

Las amenazas persistentes avanzadas (APT´s) son ataques lanzados por adversarios, estos poseen diferentes habilidades y recursos necesarios, que le permiten crear oportunidades para lograr sus objetivos mediante el uso de múltiples vectores de ataque, se aprovechan de las vulnerabilidades o debilidades a las que son expuestas.

En la Figura 5 se ilustra los principales elementos de amenaza y riesgo, los propietarios hacen referencia al propietario del activo, que son los bienes que poseen valor para la organización tangible o intangible, los riesgos tomado del ISO 27005: "Amenazas de abuso, vulnerabilidades de los activos para generar daño a la organización", que considera que el riesgo se compone de los

siguientes elementos: Activo (Vulnerabilidades y Controles), Amenaza (Agente de Amenaza, Probabilidad) e Impacto, afectan a los bienes, las amenazas son cualquier cosa que puede dañar a un bien de la organización, estas son generadas por agentes de amenazas que son adversarios que las provocan a través de vectores de ataque que son los diversos mecanismos por el cual lanzan estos ataques.

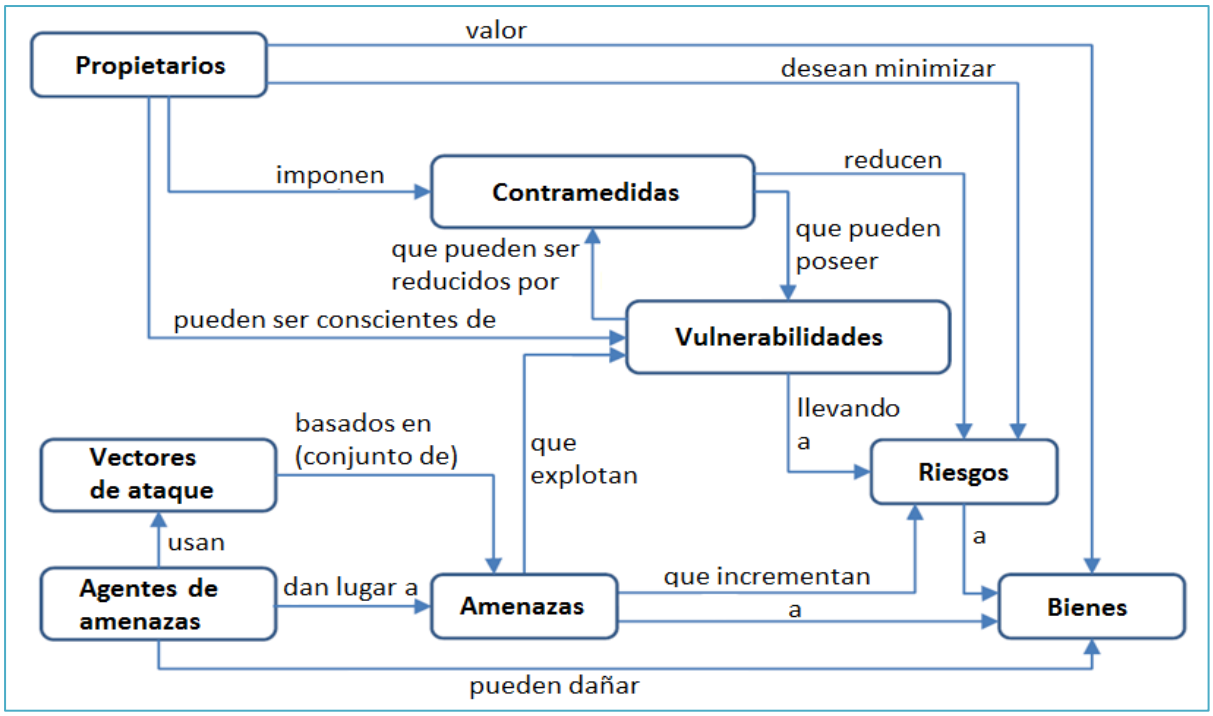


Figura 5. Elementos de amenaza, riesgo y su relación acorde al ISO 15408:2005.

Fuente: Adaptado de ENISA (2017).

2.3 COBIT 5

Cobit 5 proporciona un marco integral que dirige a las empresas hacia sus objetivos de gobernanza y Gestión de TI empresarial, creando un valor óptimo de la tecnología de la información, conservando un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y el uso de los recursos.

En noviembre del 2018 ISACA publica Cobit 2019, que maneja estándares de nube y buenas prácticas como el de Amazon Web Services (AWS), ahora se maneja los niveles de capacidad del proceso, valorados con el mismo rango del cero al cinco al igual que Cobit 5, adicionalmente se tiene los niveles de madurez del área prioritaria también valorados del cero al cinco.

2.4 Modelo de negocio para la seguridad de información

Es un modelo tridimensional (Organización, Tecnología y Personas) que permite crear oportunidades para los programas de seguridad de la información. (ISACA, 2010)

En la Figura 6 se puede identificar el modelo que se compone de cuatro elementos y tres interconexiones dinámicas, el modelo se considera en equilibrio, puesto que se distorsiona si se intercambian las partes.

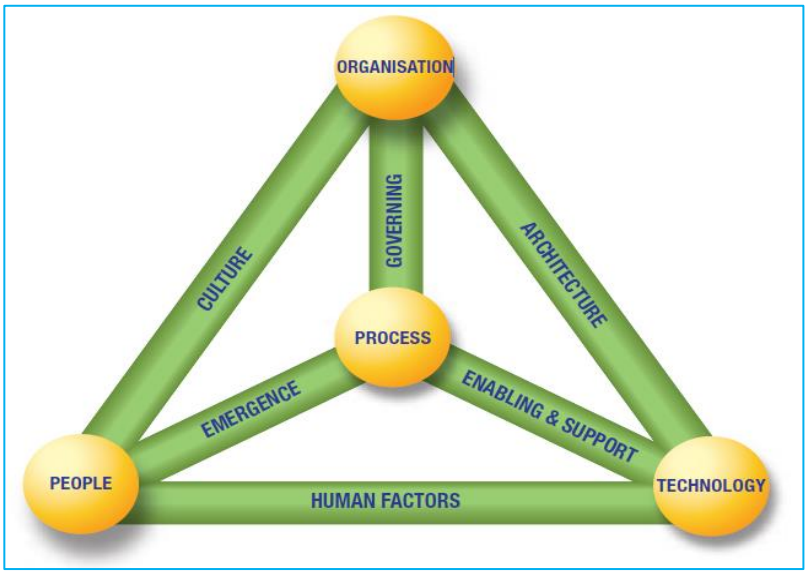


Figura 6. Visión del Modelo de Negocio para la Seguridad de Información.
Fuente: Adaptado de "The Business Model for Information Security" de ISACA (2010).

El modelo mostrado en la Figura 6 se dirige a tres elementos tradicionales considerados en TI que son: personas, procesos y tecnología, añade un cuarto elemento crítico que es la Organización.

En cuanto a las personas son un elemento importante, pero no cambian con el tiempo, se irán adaptando a los programas de seguridad. La organización es influenciada por el diseño general de la empresa y la estrategia que es requisito clave. ISACA (2010) afirma que una organización de seguridad bien diseñada puede mejorar más la situación general de riesgo de la empresa.

La tecnología hace referencia a cada aplicación de habilidad técnica y el conocimiento que podría tener un impacto en la seguridad de información, también hace referencia a otras tecnologías como aplicaciones basadas en web y almacenamiento de datos, acceso a través de redes públicas y otras tecnologías que utilizan las personas como servicios. Por otro lado, si los empleados evitan el proceso o no siguen las políticas, puede haber riesgos adicionales en la organización.

Muchas veces los procesos de seguridad, ataques internos o externos en una organización como continuos, se ven de forma lineal como ataque y reacción, si estos fueran vistos de una forma sistémica, circular, permitirán identificar relaciones de causa-efecto.

Si bien en la práctica la mayoría de estos círculos, con sus dependencias, son conocidos por profesionales de seguridad, pocas veces son formalizados o documentados.

En la Figura 7 se muestra un subsistema de seguridad, para cada acción, hay un enlace de vuelta a la estructura original, permitiendo brindar información para las acciones siguientes y detectando las causas. El total de empleados en la organización influye en el número de ataques internos que se pueda presentar, a su vez los mecanismos de ataques disponibles, que son los exploits, incrementan el total de ataques, si la empresa responde de forma sistémica, los ataques

serán detectados y apuntarán a ciertas vulnerabilidades que se identifican, a mayor cantidad de vulnerabilidades del activo, este va incrementando su valor. La falta de vigilancias o medidas conduce a un objetivo para un atacante, que incrementa su probabilidad de atacar al activo y a su vez incrementa el número de ataques en la organización. Si esto sigue así, la empresa se verá atrapada en un bucle sistémico de ataques cada vez mayores. (ISACA, 2010).

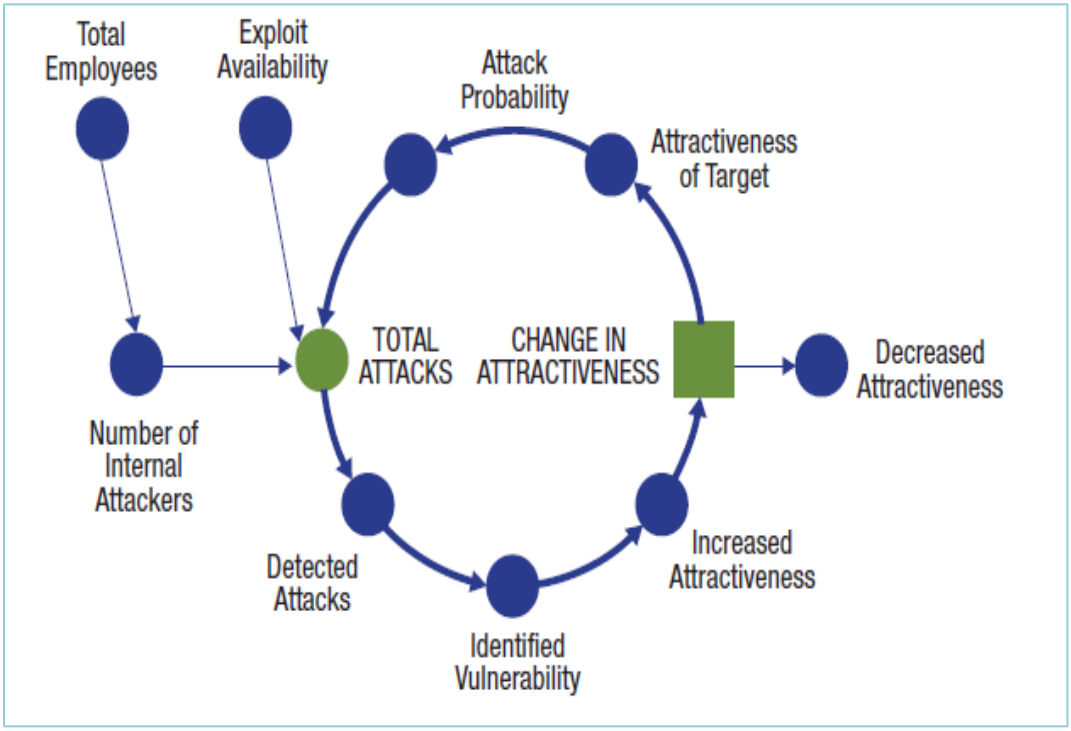


Figura 7. Ataque interno en un subsistema de seguridad.

Fuente: Adaptado de "The Business Model for Information Security" ISACA (2010).

2.5 Modelo Dinámico

Aracil (1997) define por modelo como un objeto que representa a otro, es decir como un instrumento que ayuda a un observador a describir un aspecto de la realidad que se considera como un sistema.

Guckenheimer & Ellner (2011) describen los modelos dinámicos como representaciones simplificadas de alguna entidad del mundo real en ecuaciones o códigos de computadora, que imitan las características escenciales de algún sistema de estudio y describen como cambian las propiedades del sistema en el tiempo.

Por su parte Meerschaert (2013) define modelos dinámicos como aquellas representaciones del comportamiento cambiante de un sistema.

El modelado de sistemas dinámicos se utiliza para describir y predecir las interacciones que intervienen entre las diferentes variables de un sistema a lo largo del tiempo. (Matthew & Zheng, 2017)

Un concepto bastante relacionado con el modelo dinámico es el sistema dinámico. Massachusetts Institute of Technology (MIT) (1997) define sistema dinámico como un sistema en el que las variables interactúan para estimular cambios con el tiempo y la dinámica de sistemas es una metodología utilizada para comprender estos cambios en el comportamiento del sistema.

La literatura encontrada permitió identificar muchas definciones de modelos dinámicos en diversas áreas como biología, mecámica, matemática, análisis de datos entre otros y todos coinciden que los modelos dinámicos permiten simular el comportamiento cambiante de las variables a través del tiempo. Para la presente tesis se utiliza esta definición aplicando la metodología de dinámica de sistemas.

2.6 Pensamiento Sistémico

El pensamiento sistémico es la visión completa de varios elementos y sus interacciones, que está orientado a examinar la interrelación de objetos que presentan un objetivo en común, proporciona una visión holística, abarcando una variedad de herramientas, métodos y principios.

"El pensamiento sistémico es la quinta disciplina que integra las demás disciplinas, fusionándolas en un cuerpo coherente de teoría y práctica". (Senge, 2010, p. 21)

Senge (2010) menciona que la esencia del pensamiento sistémico es ver las interrelaciones entre las variables en vez de las relaciones lineales de causa - efecto y ver los procesos de cambio. (p. 97)

Las ideas y herramientas que presenta Peter Senge (2006, 2010) están destinadas a destruir la ilusión que el mundo está compuesto por fuerzas separadas y desconectadas.

Es importante entender el concepto de sistema como el objeto formado por un conjunto de partes entre las que se establece alguna forma de relación que las articula en la unidad que es precisamente el sistema. (Aracil, 1997)

Las partes y la interacción entre ellas son los elementos básicos en esta concepción del sistema.

En el pensamiento sistémico, cada imagen cuenta una historia y se representan mediante diagramas causales. De cualquier elemento de una situación ("variable"), se pueden trazar flecha ("eslabones") que representan la influencia sobre otro elemento. A la vez éstos revelan ciclos que se repiten una y otra vez, mejorando o empeorando las situaciones. (Senge, 2006)

Existen dos elementos básicos en la configuración de todas las representaciones de sistemas: los ciclos reforzadores y los ciclos compensadores. (Senge, 2006).

Los ciclos reforzadores: Generan un crecimiento exponencial, puesto que van acumulando las variables.

Los ciclos compensadores: Generan fuerzas de resistencia que terminan por limitar el conocimiento.

2.6.1 Dinámica de Sistemas

"Método concreto para el estudio de los sistemas que forman nuestro entorno". (Aracil, 1997, p. 19)

La simulación en dinámica de sistemas permite ver en tiempo real el comportamiento de las variables añadiendo facilidades para su verificación y validación.

La dinámica de sistemas muestra de qué modo la estructura de realimentación de una organización domina la toma de decisiones por parte de los individuos.

En la Figura 8 se muestra mediante bucles de retroalimentación los distintos elementos que intervienen en la descripción del proceso. En el proceso (a), vemos que se traduce a un diagrama causal de influencias, en el que el nivel deseado aumenta la discrepancia y esta aumenta el flujo de agua que a su vez aumenta el nivel y a mayor nivel reduce la discrepancia. En el proceso (b) vemos su representación causal.

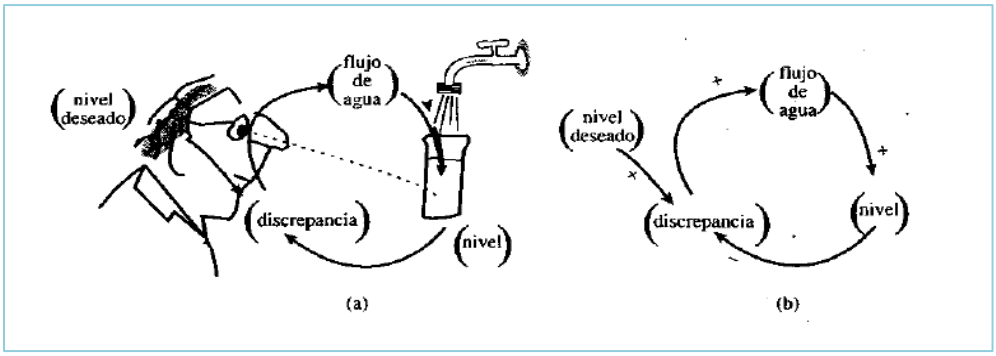


Figura 8. Proceso llenar un vaso de agua (a) con un grafo orientado (b) con un grafo signado.

Fuente: Adaptado de Aracil (1997).

2.6.1.1 Diagrama de Forrester

En la figura 9, se visualiza algunos símbolos importantes antes de realizar el diagrama de Forrester.

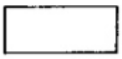
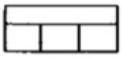
	*Nube:*	representa una fuente o un pozo; puede interpretarse como un nivel que no tiene interés y es prácticamente inagotable.
	*Estado:*	representa una acumulación de un flujo.
	*Flujo:*	variación de un nivel; representa un cambio en el estado del sistema.
	Canal de material:	canal de transmisión de una magnitud física que se conserva.
	Canal de información:	canal de transmisión de una cierta información, que no es necesario que se conserve.
	*Variable auxiliar:*	una cantidad con un cierto significado físico en el mundo real y con un tiempo de respuesta instantáneo.
	Constante:	un elemento del modelo que no cambia de valor.
	*Retraso:*	un elemento que simula retrasos en la transmisión de información o de material.
	*Variable exógena:*	variable cuya evolución es independiente de las del resto del sistema. Representa una acción del medio sobre el sistema.

Figura 9. Variables de estado utilizados en el diagrama de Forrester.

Fuente: Adaptado de Aracil (1997).

Las variables de nivel son las que van acumulando, por ejemplo, las cartas en buzones de correos, en la Fórmula 1 vemos que se representan con X, donde X (0) se asocia con un estado inicial y X (t) es el estado en función del tiempo. A las variables de nivel se le puede asociar un flujo de entrada representado por F_e y otro de salida representado por F_s como se aprecia en la Fórmula 1.

$$X(t) = X(0) + \int_0^t (F_e - F_s)\partial t$$

Fórmula 1.

Las variables de flujo son las variaciones que hay en el sistema, en la Figura 10 se puede observar su representación en el diagrama de Forrester.

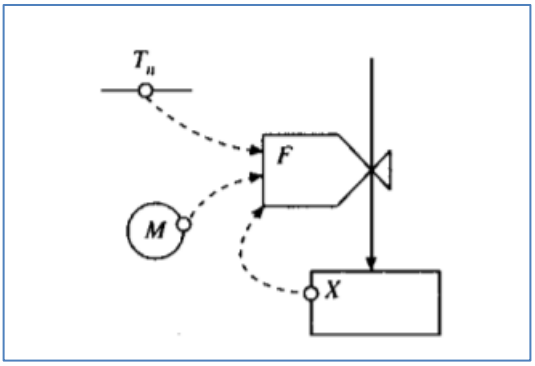


Figura 10. Representación en el diagrama de Forrester de un flujo.
Fuente: Adaptado de Aracil (1997).

En la Fórmula 2 se puede apreciar la ecuación del flujo en una forma muy frecuente de representarlo que deriva de la Fórmula 1 y acorde a la Figura 10, donde: $F(t)$ es el flujo en función del tiempo, T_n es una tasa normal, $M(t)$ es un multiplicador de flujo normal y X es un estado en función del tiempo (variable de nivel).

$$F(t) = T_n M(t) X(t)$$

Fórmula 2.

La Dinámica de Sistemas dispone de una metodología propia para el proceso de modelado y análisis que se sintetiza en las siguientes cuatro fases:

(1) Fase de identificación del problema y análisis del comportamiento.

(2) Fase del modelado cualitativo o causal, del sistema.

(3) Fase de modelado cuantitativo.

(4) Fase de evaluación y análisis del modelo.

Las dos primeras se comparten con otras disciplinas que se encuentran bajo el paraguas del Pensamiento Sistémico, como el Análisis Sistémico, pero las dos últimas son específicas y características de la Dinámica de Sistemas.

1. **Fase de identificación del problema y análisis del comportamiento**.

   En esta primera fase se debe especificar claramente el problema. A continuación, se identifica las variables clave asociadas a las magnitudes cuya variación a lo largo del tiempo queremos estudiar y que ayuden a definir los referidos límites del sistema, así como la estructura de realimentación que gobierna su dinámica.

2. **Fase del modelado cualitativo o causal del sistema**.

   En esta segunda fase se elabora una hipótesis dinámica o causal, ello implica definir las influencias que se producen entre los elementos que integran el sistema. El resultado de esta fase es el establecimiento del Diagrama de Influencias o Diagrama Causal.

3. **Fase de modelado cuantitativo.**

   En esta fase se debe disponer de un modelo matemático o Modelo Cuantitativo, del sistema para ser simulado en un computador. Para ello se debe traducir el Diagrama Causal a un Diagrama de Forrester que es un paso intermedio para la obtención de las ecuaciones matemáticas que definen el comportamiento del sistema.

4. **Fase de evaluación y análisis del modelo**.

En esta fase se somete el modelo a una serie de pruebas y análisis para evaluar su validez y calidad. Una vez que se ha construido el Modelo Cuantitativo conviene verificar, por un lado, que el conjunto de ecuaciones sistémicas no contiene errores y validar, por otro, que el modelo responde de forma fiable a las especificaciones planteadas en la fase de análisis del modelo conceptual.

CAPÍTULO 3: ESTADO DEL ARTE

El capítulo muestra una comparación de investigaciones existentes para resolver la problemática en la seguridad. Además, se describen los diferentes trabajos de investigación y artículos existentes relacionados al uso de la dinámica de sistemas en entornos vulnerables.

3.1 Criterios de búsqueda

Para la revisión de la literatura se ha realizado una búsqueda de artículos en revistas y conferencias en los bancos IEEE Xplore, ACM DL, Springer, ScienceDirec. No todas las investigaciones encontradas han sido seleccionadas para la presente tesis.

En la Tabla 5 se puede identificar los criterios de búsqueda con su respectiva ecuación de búsqueda. De los veinticuatro artículos de Springer encontrados solo uno es relevante (Kondakci, 2015), donde se evalúa modelos de confiabilidad, el modelo de ataque; de las dos siguientes búsquedas de Science Direct, ninguno; de la cuarta búsqueda de Science Direct se destaca a siete artículos , el primero de Miyamoto, Holzer, & Sarkani (2017) , utilizan la dinámica de sistemas; Boiko & Shendryk (2017) ,enfatizan la protección efectiva contra amenazas; Wang, Rho, Chen & Cai (2017), utilizan la simulación; Teixeira, Shames, Sandberg & Johansson (2015), muestran escenarios de ataque y describen las políticas para cada uno de ellos, GhasemiGol, Takabi, & Ghaemi-Bafghi (2016), proponen un modelo para gestionar las respuestas de intrusión; Tonhauser & Ristvej (2019), analizan elementos del ciberespacio para mejorar la resiliencia cibernética y Sabillon, Serra-Ruiz, Cavaller, & Cano (2016) presentan un modelo de auditoría de la ciberseguridad. También se ha realizado busqueda en la biblioteca ScieloChile.

Tabla 5. Producción científica identificada-Criterios de búsqueda (2015-2019)

(consultada el 19 de octubre de 2019).

	Ecuación de búsqueda	Science Direct	IEEE Xplore Digital Library	ACM Digital Library	Springer
Relacionado con la seguridad infraestructura de las TIC.	("security management " OR "information security" OR "cybersecurity" OR "computer security" AND "ICT infrastructure")	24	Journals (1,683) Books (123) Magazines (488) Standards (17) Early Access Articles (174) Conferences (6,973) 9,458	("security management information security" "cybersecurity" "computer security" +"ICT infrastructure") 25	15,606
Modelos relacionados con la seguridad de la infraestructura de las TIC	("security management " OR "information security" OR "cybersecurity" OR "computer security" AND "ICT infrastructure" AND "model")	23	Journals (1,682) Books (123) Magazines (488) Standards (17) Early Access Articles (174) Conferences (6,971) 9,476	("security management information security" "cybersecurity" "computer security" +"ICT infrastructure" +"model") 9	13,482
Modelos dinámicos relacionado con la seguridad de la infraestructura de las TIC	("security management " OR "information security" OR "cybersecurity" OR "computer security" AND "ICT infrastructure" AND ("system dynamics" OR "dynamic model"))	2	Journals (1,682) Books (123) Magazines (488) Standards (17) Early Access Articles (174) Conferences (6,971) 9,477	("security management information security" "cybersecurity" "computer security" +"ICT infrastructure" +"system dynamics" +"dynamic model") 0	3,990
Modelos dinámicos relacionados con la seguridad.	("security management " OR "information security" OR "cybersecurity" OR "computer security" AND ("system dynamics" OR "dynamic model"))	53	Journals (3,092) Books (178) Magazines (1,688) Standards (35) Early Access Articles (174) Conferences (26,418) 31,616	2	338,300

Para la selección de documentos se aplicaron criterios de inclusión y exclusión que se presenta en la Tabla 6.

Tabla 6. Criterios de inclusión y excusión.

Inclusión	Exclusión
Investigaciones relacionadas con la gestión de la seguridad infraestructura de las TIC.	Modelos que no se encuentran dentro del periodo de búsqueda establecido.
Modelos relacionados con la gestión de la seguridad de la infraestructura de las TIC	Modelos basados en algoritmos de optimización.
Modelos dinámicos relacionado con la gestión de seguridad de la infraestructura de las TIC	Modelos dinámicos no relacionados con la gestión de la seguridad en la infraestructura de las TIC.
Modelos dinámicos relacionados con la gestión de la seguridad.	Trabajos que no se basan con el área de seguridad de la información, seguridad informática, ciberseguridad o ciencias de la computación.

3.2 Modelos en seguridad de la información

3.2.1 Modelo de Confiabilidad

Se busca aspectos cuantitativos, la probabilidad, estadísticos, procesos estocásticos, son candidatos para modelar ataques.

3.2.2 Modelo de Acceso

Estos modelos buscan proteger la información y activos de TIC.

3.2.3 Modelo de Auditoría

Ayuda a la evaluación de procesos corporativos, enfatizada los dominios y controles.

3.2.4 Modelo Dinámico para la Gestión de Seguridad

Tienen mayor aproximación a la realidad, capacidad de observar una serie de escenarios, ya que muchos aspectos de la seguridad de la información son dinámicos.

3.3 Evaluación Comparativa

A continuación, se muestran los factores que se tomarán en cuenta para el presente modelo:

- Adaptabilidad: Es importante que el modelo se pueda adaptar ante los diferentes escenarios de la organización.
- Eficacia: El modelo debe determinar en qué estado se encuentra nuestra organización y cuan expuestos estamos a sufrir ataques.
- Eficiencia: Resulta primordial que se pueda gestionar eficientemente las vulnerabilidades que tiene nuestra organización en el menor tiempo.
- Visibilidad: En determinado instante deseamos tener un panorama global de cómo se encuentra nuestra organización y que pasaría si no tomamos decisiones a tiempo.
- Integración: Se debe tener en cuenta la integración de las variables involucradas.

Criterios de peso a los factores:

- Adaptabilidad: Este factor presenta peso 0.2 porque que se considera importante que el modelo se pueda adaptar ante diferentes circunstancias de la organización.
- Eficacia: Este factor presenta peso 0.2 es necesario determinar el estado en que se encuentra la organización para poder gestionar la seguridad estratégicamente.

- Eficiencia: Este factor presenta peso 0.2 porque es necesario que se pueda observar el comportamiento del modelo en el menor tiempo, ante los diferentes escenarios que se presenten en la organización.
- Visibilidad: Este factor presenta peso 0.2 es importante ver resultados en determinados instantes.
- Integración: Este factor presenta peso 0.2 resulta primordial entender globalmente todas las variables involucradas.

Tabla 7. Benchmarking. Matriz de evaluación de los modelos.

MODELOS		Modelo de Confiabilidad		Modelo de Acceso		Modelo de auditoría		Modelo Dinámico para la Gestión de Seguridad	
FACTORES	**Peso**	Valor	Ponderado	Valor	Ponderado	Valor	Ponderado	Valor	Ponderado
Adaptabilidad	**0.2**	1	0.2	1	0.2	2	0.4	3	0.6
Eficacia	**0.2**	2	0.4	2	0.4	3	0.6	3	0.6
Eficiencia	**0.2**	2	0.4	2	0.4	2	0.4	3	0.6
Visibilidad	**0.2**	1	0.2	2	0.4	2	0.4	3	0.6
Integración	**0.2**	3	0.6	3	0.6	1	0.2	3	0.6
Total	1	9	1.8	10	2	10	2	18	3

En la Tabla 7 se puede evidenciar que por cada modelo hay un valor donde:

- 0: No aplica al factor.
- 1: Bajo Nivel para el factor.
- 2: Medio Nivel para ese factor.
- 3: Alto nivel para ese factor.

Resultado:

De la Tabla 7 se puede observar que se opta por un "Modelo Dinámico para la Gestión de Seguridad", puesto que es el que tiene mayor valor frente a los otros modelos.

3.4 Aplicaciones usando dinámica de sistemas en seguridad

A continuación, se presenta diferentes artículos que aplican la dinámica de sistemas para la protección en entornos de ataques y amenazas.

3.4.1 Evaluación del impacto económico debido a los ataques cibernéticos con enfoque de dinámica de sistemas.

(Roumani, Fung, & Choejey, 2015)

Los autores consideran el enfoque de dinámica de sistemas como efectivo, plantean un modelo basado en la dinámica de sistemas, para evaluar el impacto económico que podría resultar, enfatizan las pérdidas debidas a los ciberataques.

Consideran que el modelo no puede ser apropiado para situaciones complejas, puesto que se han basado en supuestos.

Destacan que la seguridad tiene un parte principal que es la seguridad inherente y otras tres secuenciales que son la seguridad preventiva, seguridad detectiva y la seguridad correctiva y recuperación.

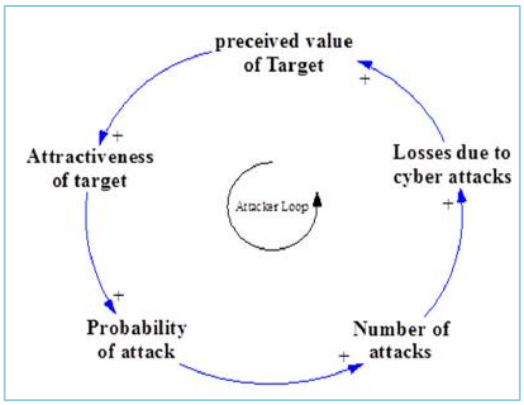


Figura 11. Lazo del atacante.

Fuente: Adaptado de (Roumani, Che, Choejey ,2015).

En la Figura 11 se observa un bucle en el cual muestra como las pérdidas afectan al valor de los activos para los atacantes.

Su importancia del presente artículo para la tesis radica en la aplicación de la dinámica de sistemas para adoptar temas como el equilibrio entre inversiones y pérdidas por ciberataques, que concientiza a los encargados de seguridad, que aspectos claves se debería considerar para salvaguardar sus activos.

3.4.2 Dinámica de redes sociales de amenazas internas: un modelo preliminar.

(Moore, Carley, Collins, & Altman, 2015)

Los autores proponen un modelo que permita a los gerentes pensar en quién podrían convertirse en amenaza, rastrear hallazgos del análisis de datos y proporcionar el potencial para evaluar los beneficios de la organización, medidas para mejorar el capital social de los empleados.

Su importancia radica en las motivaciones de espionaje, si bien el capital social bajo dentro de la organización puede ser un factor en la información privilegiada con decisión de espiar, las

motivaciones más tradicionales incluyen dinero, ideología, compromiso, coerción, así como el desafecto y las relaciones personales con individuos de influencia.

Para ello se describen dos casos de directores de los EE. UU., que publicaron información confidencial de su organización, uno para disfrutar de un estilo de vida acomodado y el otro por motivaciones ideológicas.

El presente modelo simula los mecanismos que podrían promover o reflejar la decisión de un iniciado (trabajador de la organización) de cometer un acto malicioso en términos de las redes sociales.

Destacan tres factores para identificar a los actores que son amenazas potenciales: cultura organizacional, personalidad y distanciamiento social, a su vez desarrollan una medida de motivación interna basada en las cuatro variables de motivación de Stone, las variables oscilan entre 0 y 1, tanto a niveles de motivaciones de dinero, ideología, desafíos y coerción.

Considera tres redes sociales primarias dentro del cual el capital social puede crecer o declinar: la organización (víctima), el adversario (no estadounidense actor estatal) y la familia del espía.

Los autores utilizaron la herramienta Vensim® PLE, planteando dos submodelos uno referido al crecimiento del capital social organizacional y el otro referido al adversario y capital social de la familia.

El presente modelo muestra que, si bien un nivel medio de la motivación de la persona en una sola dimensión no es suficiente para estimular el espionaje, en si ya representase un alto nivel de motivación.

Además, un nivel medio de motivación a través de atributos motivacionales ortogonales puede estimular espionaje (por ejemplo, un nivel medio de desafección, así como un nivel ideológico de motivación).

Este artículo contribuye a la presente tesis puesto que muestra de forma preventiva los factores de divulgación de información confidencial de una organización vista de un entorno dinámico, ayudarían a mejorar la gestión de la seguridad.

3.4.3 Un enfoque de dinámica del sistema para evaluar el impacto de los ciberataques en las infraestructuras críticas.

(Bela, Kiss, & Piroska, 2015)

Los autores se enfocan en el problema de cómo saber los impactos de ciberataques en infraestructuras críticas ya que existe una gran variedad de ciberataques y posibles implementaciones.

Para ello abordan dos temas: la dinámica de sistemas y análisis de sensibilidad, desarrollando una metodología en cual consideran la arquitectura de una infraestructura crítica y el uso de la metodología Cyber Attack Impact Assessment (CAIA), evaluación de impacto del Cyber Attack, que incorpora un ataque cibernético y lo compara el comportamiento de procesos físicos complejos en presencia y ausencia de accidentes o intervenciones deliberadas para evaluar la importancia de los activos cibernéticos.

Para ello considera la arquitectura de la infraestructura que comprende 2 capas: (1) capa física, que abarca sensores, actuadores y hardware dispositivos que interactúan con los procesos físicos; (2) y la ciber-capa, que abarca la tecnología de la información y las comunicaciones.

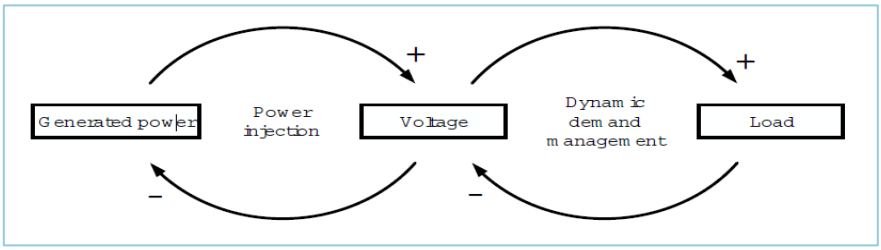


Figura 12. Diagrama causal de una red de energía eléctrica.

Fuente: Adaptado de (Bela, Kiss, & Piroska, 2015).

La Figura 12 muestra un ejemplo de diagrama de bucle causal para un escenario simplificado envolviendo a una red de energía eléctrica. "El nexo causal positivo entre los generados los niveles de voltaje de la energía y la subestación denota que los cambios en el generado el resultado de la potencia en el nivel de voltaje cambian en la misma dirección (aumentar o disminuir). Por otro lado, el nexo causal negativo entre voltaje y la potencia generada denota que el voltaje aumenta (por encima de ciertos límites)." Adaptado de (Bela, Kiss, & Piroska, 2015)

La metodología compara el comportamiento de procesos físicos complejos en presencia y ausencia de accidentes o intervenciones deliberadas para evaluar la importancia de los activos cibernéticos, es aplicable a gran escala, instalaciones jerárquicas y heterogéneas, pero lo más importante, puede ser utilizado para evaluar los impactos de las perturbaciones como la causadas por ciberataques en una variedad de sistemas de producción.

El presente artículo contribuye a la tesis puesto que se analiza el impacto que puede generar un ataque en una infraestructura, para nuestro caso que es de una organización tecnológica es importante la infraestructura de la organización.

3.4.4 Mecanismo de defensa de botnet HTTP utilizando algoritmos genéticos basados en dinámicas de sistemas.

(Mathew & Pauline, 2016)

Los autores consideran la dificultad de detectar los ataques Botnet, puesto que para su comunicación utilizan el protocolo HTTP y estos presentan características muy similares a otros tráficos ordinarios como el TCP.

La importancia radica que los aumentos de los ciberataques se ven encausados por las Botnets, estas ponen en peligro la seguridad, pues son una colección de sistemas comprometidos bajo el control de un Bot master.

El sistema propuesto hace uso de algoritmos genéticos basados en dinámica de sistemas para la defensa HTTP botnet.

Inicialmente se tiene la detección por capas basada en algoritmos genéticos, que consiste en un grupo de clasificación, esta se configura seleccionando los valores aleatoriamente. Pero solo puede asegurar menos tasa de falsos positivos.

A través de los experimentos se demostró que el mecanismo de defensa HTTP Botnet de dinámica de sistemas basado en algoritmos genéticos se considera la dinámica del atacante, esto produce una eficiente detección.

El aporte del presente artículo está en que mediante enfoque de dinámica de sistemas podemos llegar a la eficiencia en la detección de las amenazas.

3.4.5 Enfoque de dinámica del sistema para el análisis y modelado de amenazas cibernéticas internas maliciosas.

(Fagade, Spyridopoulos, Albishry, & Tryfonas, 2017)

Los autores plantean la dificultad de las organizaciones por reforzar sus capacidades cibernéticas, el incremento de personas mal intencionadas y las numerosas soluciones asociadas a las personas, procesos y tecnología, tornan difíciles de aplicar en grandes sistemas complejos.

Los autores aplican el modelado de dinámica de sistemas para comprender las interrelaciones entre tres indicadores distintivos de una persona interna maliciosa, con el fin de determinar la posibilidad de una brecha de seguridad a través del desarrollo de tendencias y patrones; estas son: el comportamiento del observador; las huellas técnicas de información de los registros de incidentes y la red social para conocer el perfil de los rasgos de personalidad.

En su aporte combinan dos modelos: el modelo conductual y el psicológico; captan los perfiles observables de la personalidad de los actores a través de huellas de redes sociales y pistas de auditoría del sistema establecidas a partir de información de registro de incidentes de recursos de TI. Para ello utilizó la herramienta Vensim PLE que es un software de dinámica de sistemas.

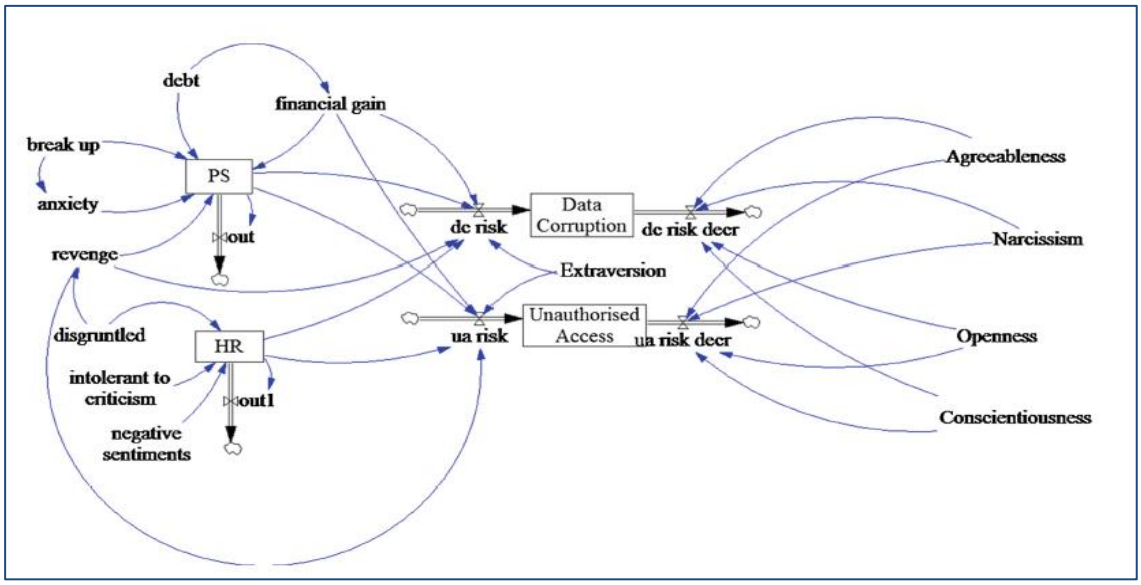


Figura 13. Relación dinámica entre la personalidad, comportamiento e incidentes de seguridad cibernética.

Fuente: Adaptado de (Fagade, Spyridopoulos, Albishry, & Tryfonas, 2017).

El modelo de Forrester describe la dinámica entre el comportamiento, la personalidad y la probabilidad de una persona incidente de seguridad cibernética (corrupción de datos o acceso no autorizado), el comportamiento está considerado como la combinación del estado psicosocial (PS) de una persona, dada por factores externos (ejemplo, ruptura o deuda), con el comportamiento interno del empleado (ejemplo, intolerancia a la crítica o sentimientos negativos). El comportamiento interno negativo combinado con un estado psicosocial no saludable puede aumentar la probabilidad de un incidente de seguridad cibernética y donde el análisis conductual combinado (HR) sirve para los perfiles de seguridad interna, como se muestra en la Figura 13.

En el presente modelo aporta puesto que demuestra cómo la dinámica de sistemas puede marcar los primeros signos de problemas internos maliciosos, basado en las propiedades asociativas de diferentes elementos de riesgo.

3.4.6 Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas.

(Parada, Flórez, & Gómez, 2018)

Los autores presentan la propuesta de un modelo que permite medir la seguridad de la información relacionando la complejidad de los diferentes elementos involucrados, presentando como resultado que los controles juegan un papel fundamental en la valoración de los activos, en un escenario sin controles se puede apreciar la materialización del riesgo de los activos.

Consideran que la seguridad está compuesta de siete elementos fundamentales: los interesados, los activos, las vulnerabilidades, el riesgo, los controles, las amenazas y los agentes de amenaza (atacantes o intrusos).

El presente artículo contribuye a la tesis puesto muestra la interacción entre los diferentes elementos que involucran a la seguridad (Figura 14). Mencionan cinco bucles el primero, Activos-Atacantes-Amenazas-Materialización-Riesgo-Impacto-Activos; el segundo, Activos-Vulnerabilidades-Materialización-Riesgo-Impacto-Activos; el tercero, Activos-Riesgo-Impacto-Activo; el cuarto, Activos-Controles-Materialización-Riesgo-Impacto sobre los Activos; el quinto, Riesgo-Impacto-Controles-Materialización-Riesgo.

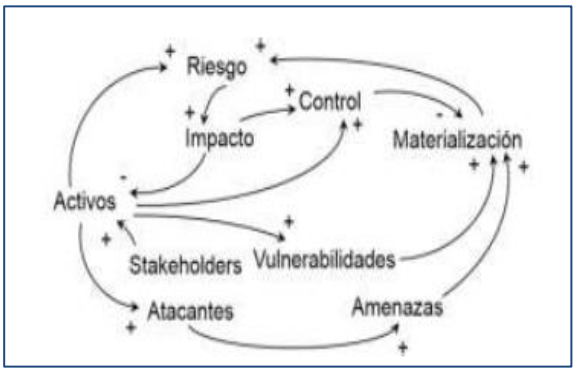


Figura 14: Diagrama de influencias de los componentes de seguridad.

Fuente: Adaptado de (Parada, Flores, Gómez, 2018).

En la Tabla 8 se puede evidenciar una evaluación de las investigaciones usando dinámica de sistemas en seguridad antes detallados, bajo dos premisas ¿Qué aspecto considera importante que abarca este enfoque? y ¿Qué problema enfatizan?, nos damos cuenta de que abarcan los factores considerados en el Benchmarking, además observamos que la dinámica de sistemas puede ser aplicada para resolver diferentes tipos de problemáticas en seguridad.

Tabla 8. Evaluación de la producción científica seleccionada en dinámica de sistemas.

Enfoque de dinámica de sistemas / (system dynamics)

	(Roumani, Fung, & Choejey, 2015)	(Moore, Carley, Collins, & Altman, 2015)	(Bela, Kiss, & Piroska, 2015)	(Mathew & Pauline, 2016)	(Fagade, Spyridopoulos, Albishry, & Tryfonas, 2017)	(Parada, Flórez, & Gómez, 2018)
¿Qué aspecto considera importante que abarca este enfoque?	Efectividad.	Proporciona potencial para evaluar beneficios, pensar en posibles amenazas, rastrear hallazgos. (Visibilidad)	Ayuda a analizar el impacto que puede generar el ataque hacia una infraestructura.	Eficiencia en detección.	Ayuda a comprender las interrelaciones. (Integración)	Ayuda a visualizar los componentes involucrados en Seguridad.
¿Qué problema enfatizan?	Pérdida por ciberataques.	Motivaciones de espionaje.	Impactos de ciberataques en infraestructuras críticas.	Dificultad de detectar los ataques Botnet.	Dificultad de las organizaciones por reforzar sus capacidades cibernéticas.	Medir la seguridad con los diferentes elementos involucrados.

CAPÍTULO 4: DESARROLLO DEL MODELO DINÁMICO

De acuerdo con el estado del arte se observa que en problemas similares al que enfrentamos se ha optado por soluciones que apuntan a resolver aspectos de tipo:

- Inversión en seguridad.
- Control de accesos.
- Políticas

Varios de ellos solo abarcan parte de la problemática, dejándose de atender aspectos de tipo:

- Adaptabilidad.
- Visibilidad.

El problema difiere de los anteriores puesto que se busca una mayor visibilidad y adaptabilidad de las variables involucradas, proyectarse en diferentes escenarios de la organización, predecir en un determinado instante de tiempo en qué panorama se encuentra la organización, muchas veces se deja de lado aspectos importantes.

En el modelo dinámico toma en cuenta aspectos globales basados en reportes internaciones publicadas y aspectos propios de cada organización con los niveles de capacidad de Cobit 5 y la ISO 27001.

Por tanto, se busca gestionar adecuadamente la seguridad de la infraestructura de las TIC, detectando las vulnerabilidades y amenazas a tiempo, bajo el escenario al que está expuesto la organización, se toma el estudio con el enfoque de dinámica de sistemas, para ello se utilizó la herramienta Vensim® PLE.

4.1 Análisis de la solución

La construcción de la solución como ya se indicó utilizará la metodología propia de Dinámica de Sistemas.

Se logrará un modelo proactivo a nivel de la seguridad y permitirá alcanzar una proyección a futuro de cuan protegido se encuentre.

La metodología consta de los siguientes procedimientos:

- Identificar las variables asociadas.

Primero se realiza un análisis de la organización acerca de cómo se encuentra el área, que aspectos consideran importante los encargados de seguridad para la toma de decisiones.

- Realizar el modelo causal.

Luego se procede a identificar la relación de las variables asociadas a través de lazos causales y la realimentación entre ellas, completando una visión sistémica de causa efecto.

- Realizar el modelado cuantitativo.

Consiste en la construcción Diagrama de Forrester a partir del modelo causal, obteniendo ecuaciones matemáticas que definan el comportamiento del sistema, viendo las relaciones entre variables de nivel, variables de flujo y las variables auxiliares.

- Evaluación y análisis del modelo

Se comprueba la consistencia lógica en las corridas del modelo, bajo los diferentes escenarios.

Descomposición del proceso

Para el caso de estudio se considera el proceso de Seguridad de la infraestructura tecnológica, redes y comunicaciones en una entidad financiera que por motivos de confidencialidad será denominada como "Empresa A".

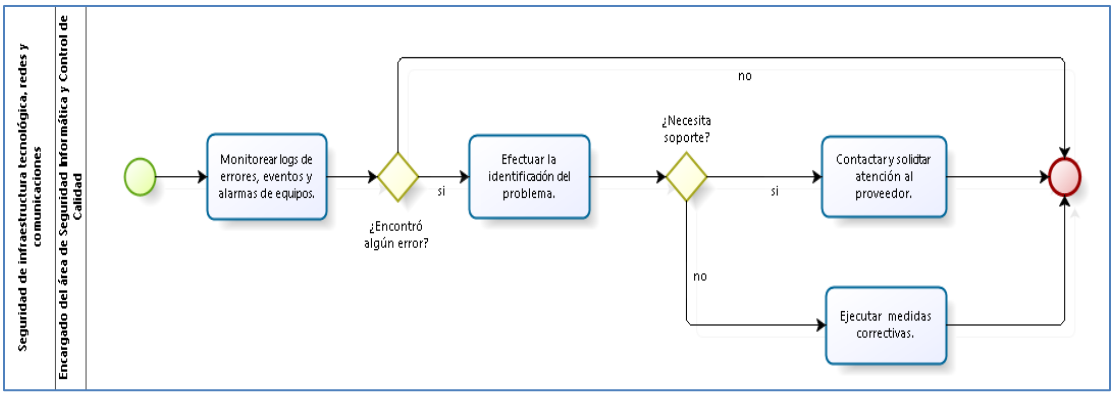


Figura 15. Seguridad de la infraestructura tecnológica, redes y comunicaciones.

En la Figura 15 se observa que primero el encargado del área de seguridad informática monitorea logs de errores, eventos y alarmas en los equipos de comunicaciones.

Si encontró algún error, procede a efectuar la identificación del problema, si no, termina el proceso, si necesita soporte, se contacta y solicita atención al proveedor, si no se ejecutan medidas correctivas que permiten solucionar el problema, redactando un informe hacia el jefe de sección de infraestructura tecnológica y termina el proceso. Si solicita atención del proveedor, se contacta con este y solicita un informe de atención del proveedor dando fin al procedimiento.

4.2 Análisis de la problemática

La infraestructura de la Empresa A está expuesta a ataques que buscan vulnerar sus activos, ello conlleva a riesgos en seguridad que se ven materializados en pérdidas para la empresa, actualmente la Empresa A no cuenta con una herramienta que le permita gestionar y ver en tiempo

real como está su nivel de seguridad, que decisiones adecuadas tomar que le permita proyectarse a futuro en diferentes escenarios.

Cuando ocurre un ataque lo primero que realizan es sacar de la red aquel equipo comprometido para que no afecte a los demás, poniéndolo en otra red alternativa para observar su comportamiento, ahí estamos viendo posibilidades, mientras tanto la organización no puede parar, debe seguir operando y continuidad del negocio se encarga de ello, sabemos que existen herramientas y equipos que bloquean dichos ataques, como la de Cisco Talos Intelligence Group que recopila toda la información de las vulnerabilidades que van apareciendo, el Malware Information Sharing Platform (MISP), que es una plataforma de inteligencia de amenazas de código abierto y estándares abiertos para el intercambio de información sobre amenazas, en la página del Computer Emergency Response Team (CERT) vemos alertas de las vulnerabilidades de diversas partes del mundo, IBM X-Force Exchange que es una plataforma para compartir inteligencia sobre amenazas que se puede utilizar para investigar sobre amenazas de seguridad, que proporcionan gran cantidad de información para evaluaciones de seguridad y sirven de retroalimentación para el modelo.

Estas herramientas permiten ver la inteligencia de las amenazas, ataques que se encuentran enlazados con las plataformas que los proveedores venden; pero no se tiene el recurso necesario para adquirirlas, esto conlleva a un gran nivel de riesgo que experimenta la Empresa A por la antigüedad tecnológica.

Por ello resulta importante ver desde el punto de vista del atacante que vulnerabilidad hay en la organización y como la explotaría, que daños originaría dentro de nuestra organización, como la pérdida de información, daños de imagen, daños de clientes, multas, sanciones, publicación y extorsión.

Cisco (2017), en su reporte semestral de seguridad menciona que "Las empresas de la industria financiera son objetivos lucrativos para los criminales en línea. La riqueza de los datos financieros de los clientes, más el acceso a los nombres de usuario y contraseñas de las cuentas, alientan a los agresores a lanzar una serie de ataques a las compañías del sector. De hecho, algunos creadores de malware diseñan sus embestidas específicamente para comprometer las redes de servicios de finanzas". (p . 80)

En la Figura 16, Cisco (2017) en su reporte semestral informa que "el 79%, de los casi 110,000 servidores Memcached expuestos, aún era sensible a las debilidades de ejecución remota de código." (p. 5), Además, "sólo el 22% de los servidores cuenta con la autenticación habilitada; y virtualmente, todos los sistemas seguían siendo vulnerables (23,707 de 23,907)". (p . 55)

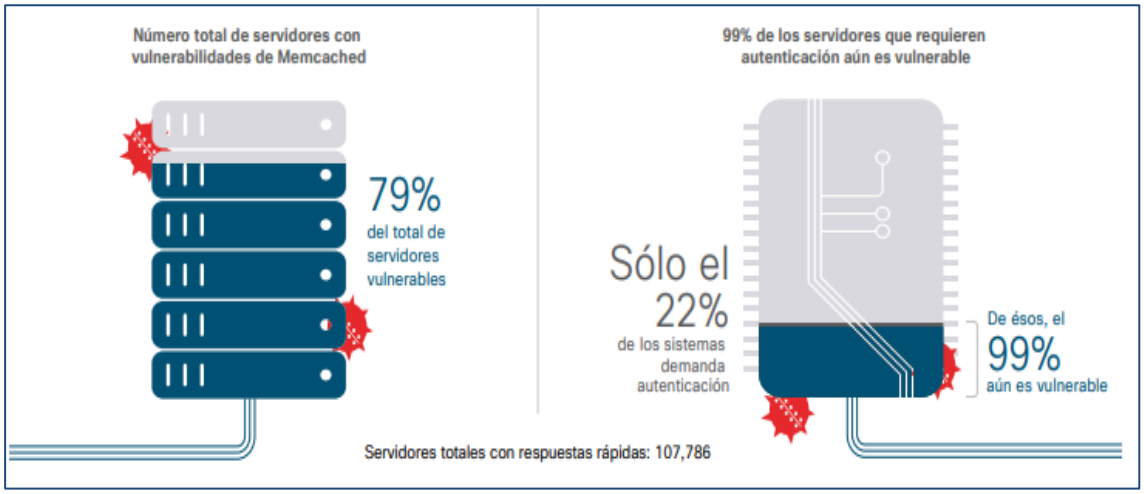


Figura 16. Servidores comprometidos.
Fuente: Cisco (2017).

Asimismo, en marzo del 2018 X-Force de IBM reportó entre las 5 principales industrias más frecuente de incidente y ataque, fueron las de servicios financieros y de tecnología de Información y Comunicaciones, como se aprecia en la Figura 16.

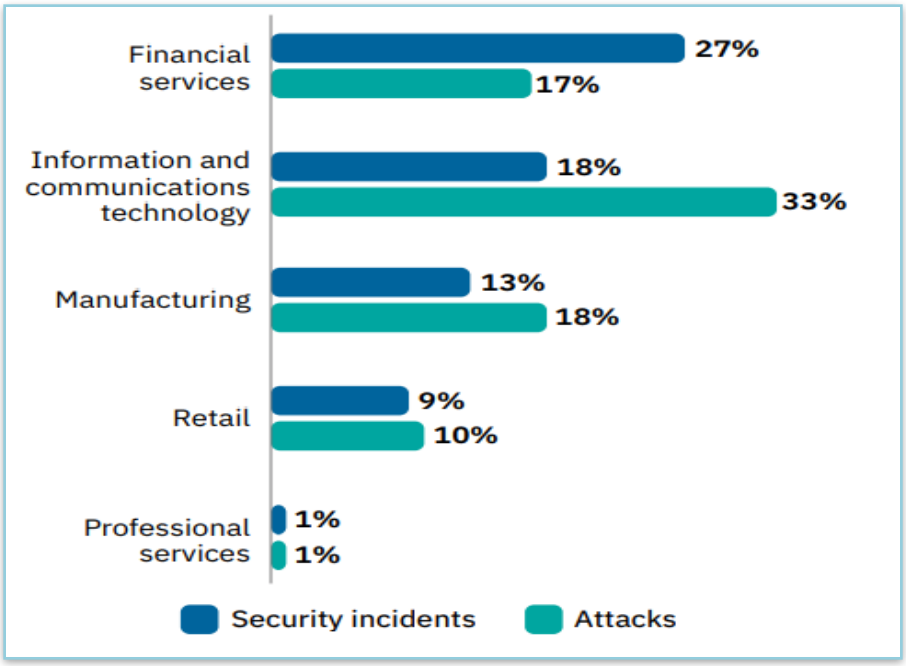


Figura 17. Porcentaje de incidentes y ataques de seguridad en 2017.
Fuente: IBM (2018).

En la Figura 17 se puede identificar que a pesar de que las empresas de tecnologías de información y comunicación experimentaron mayor cantidad de ataques, las empresas de servicios financieros experimentaron mayor cantidad de incidentes de seguridad, lo que demuestra el valor que tiene para un atacante es superior en este tipo de industrias, por tanto, se ve más comprometida en cuanto a su seguridad.

Continuando con la metodología de dinámica de sistemas se va a entender a la organización como primera etapa para la identificación de las variables que van a ingresar en el modelo dinámico, luego la realización del modelo causal, modelo cuantitativo, la evaluación y análisis del modelo.

Algunos procesos importantes con la que cuenta la "Empresa A" se muestra en la Tabla 9.

Tabla 9. Inventario de Procesos de la División de Tecnología.

Proceso	Objetivo del Proceso	Responsable
Gestión de Requerimientos	Brindar un servicio centralizado de calidad que satisfaga las necesidades de los usuarios.	Encargado del área de Sección de Planificación y Control
Gestión de Cambios de TI	Realizar e implementar adecuadamente todos los cambios necesarios en la infraestructura y servicios de TI, garantizando el seguimiento de procedimientos estándar.	Encargado del área de Producción de Sistemas y Jefe de Seguridad Informática y Control de Calidad.
Gestión de Servicios de TI	Gestionar los Servicios de tecnología de la información en base a los procesos, enfocados en alinear los servicios de TI, proporcionados con las necesidades de las empresas.	Encargado del área de Producción de Sistemas.
Gestión de Seguridad de TI	Mantener la integridad de la información y proteger los activos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados	Encargado del área de Seguridad Informática y Control de Calidad.

De acuerdo con el análisis de la solución resulta sumamente importante un modelo dinámico de gestión de seguridad con una visión holística que ayude a las organizaciones a frenar los daños que ocasionan los ataques, el monitoreo de la seguridad en la infraestructura de las TIC es primordial puesto que es uno de los aspectos que ocasiona mayor pérdida en la organización.

Para la construcción del modelo se tomó como base el comportamiento un ataque interno en la organización, sacado del BMIS (2010), aspectos de la ISO 27001 (2014), el PAM de Cobit 5 (2013), reportes internacionales y la validación de tres expertos en seguridad de redes, aplicaciones y gestión para la creación de los diferentes entornos.

4.3 Identificación de variables

En la Tabla 10 se puede distinguir las diecinueve variables identificadas para el modelo acorde a los controles de Seguridad de la Información que maneja con Seguridad Informática, esto servirá de base para la elaboración del modelo cualitativo.

Tabla 10**.** Tabla de variables identificadas para el modelo.

Variable	Descripción de la variable
Vulnerabilidades	Debilidad de un activo o control que puede ser aprovechada por una amenaza.
Ataques	Resultado de una acción reactiva de un equipo de seguridad.
Alertas de Seguridad	Indicación que un sistema de información y una red pueden estar bajo ataque o en peligro por un accidente, fallo o error humano.
Control	Salvaguardia o contramedida, medio de gestión de riesgos.
Vulnerabilidades mitigadas	Vulnerabilidades que se han aplicado controles.
Total de ataques	Resultado de varias acciones reactivas de un equipo de seguridad, acumulativo.
Ataques mitigados	Resultado de controles de equipos de seguridad y buenas prácticas.
Flujo de alertas de seguridad	Alertas de los equipos de seguridad y cómputo.
Alertas remediadas	Alertas que han sido controladas.
Nivel de capacidad	Valor dado por el Cobit 5.
Probabilidad de ataque	Grado de ocurrencia de un ataque.
Tasa de ataques mitigados	Porcentaje de ataques que mitigan los equipos de seguridad.
Planificación del cumplimiento de políticas	Número de políticas que se pretende cumplir.
Tasa de incumplimiento del control	Porcentaje de incumplimiento del control.
Tasa de alertas de seguridad confirmadas	Porcentaje de alertas que son por falsos dispositivos.
Tasa de remediación de alertas de seguridad confirmadas	Porcentaje de remediación de alertas que no son por falsos dispositivos.
Trabajadores con acceso a red	Número de trabajadores con accesos a red.
Exploits disponibles	Uso de vulnerabilidades aprovechadas por atacantes.
Amenazas de seguridad	Elemento que es capaz de producir daño a un activo.

4.4 Modelado cualitativo

Para la presente tesis se considera que las variables de color rojo son variables de nivel, las de color azul son variables de flujo y las de color negro son variables auxiliares. (Figura 18)

Además, se asume que la empresa cuenta de equipos de seguridad para protegerse de los diferentes ataques. En base a los indicadores definidos anteriormente, se plantea el siguiente diagrama causal que se muestra en la Figura 18.

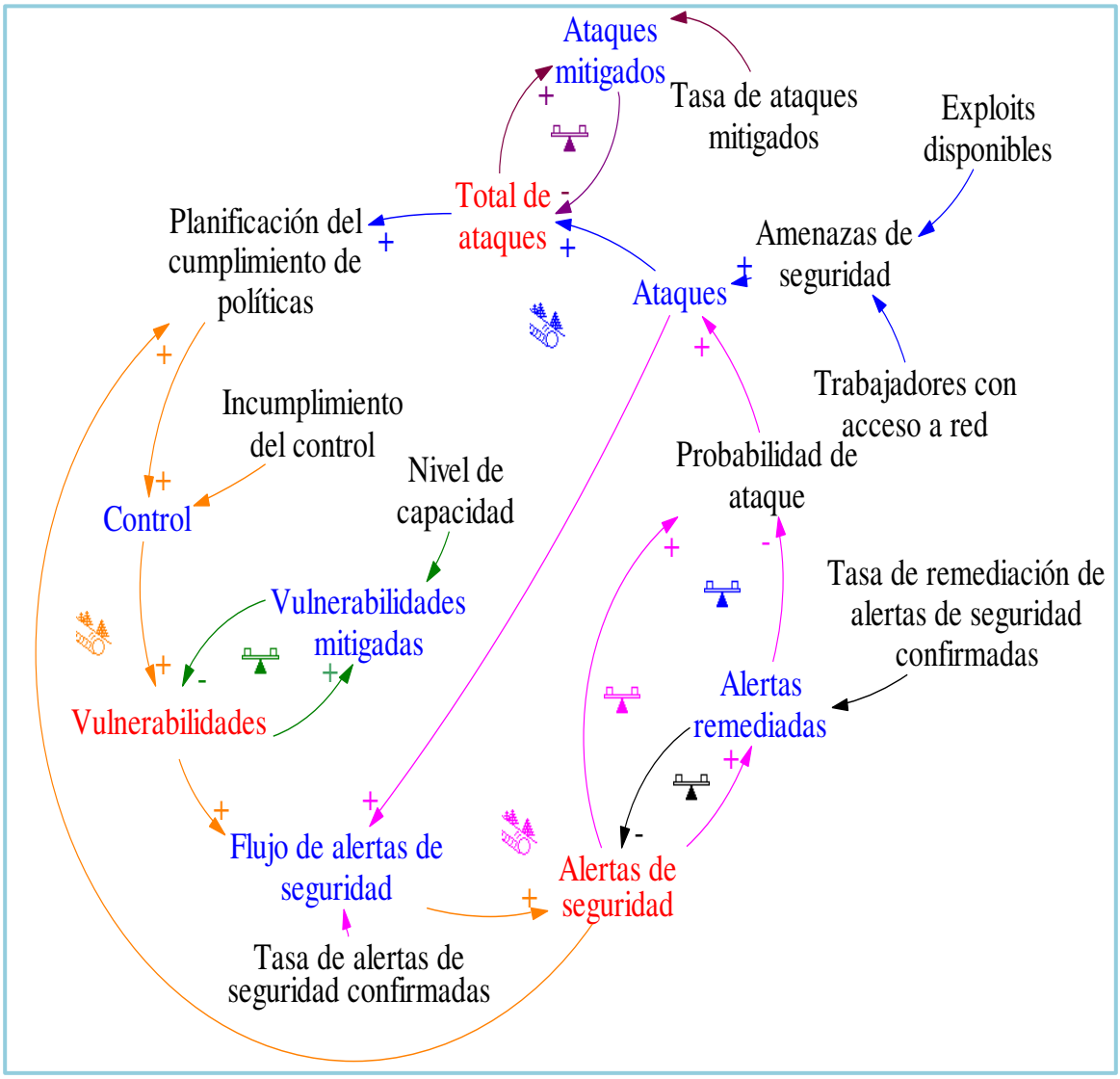


Figura 18. Modelo causal de seguridad.

A continuación, se detalla cada uno de los bucles de influencias del modelo causal.

Bucle reforzador:

Bucle 1: Ataques - Flujo de alertas de seguridad - Alertas de seguridad - Probabilidad de ataques - Ataques

En el modelo causal Figura 18, podemos apreciar en el bucle reforzador de color fucsia que como efecto de un ataque se genera una alerta de seguridad, entonces a mayor cantidad de ataques tenemos más alertas de seguridad; pero estas alertas no son solo reactivas , también pueden ser preventivas, como una actualización de versión, entonces el flujo de alertas de seguridad viene influenciado por dos variables los ataques (reactivo) y las vulnerabilidades existentes (preventivo), sabemos que en las áreas de seguridad informática se tienen también alertas por falsos dispositivos, que son falsas alertas que brindan los equipos de seguridad y generan inversión de tiempo por parte de los encargados, Cisco (2017) en su reporte semestral muestra la tasa de alertas de seguridad confirmadas (que no son falsos dispositivos),entonces vamos a filtrar aquellas alertas que no sean por falsos dispositivos (flujo de alertas de seguridad), estas van a incrementar las alertas de seguridad que si no han sido remediadas (vulnerabilidad identificada) van a incrementar la probabilidad de ataque y si tenemos amenazas de seguridad que explotan vulnerabilidades entonces aumentan los ataques . (ISACA, 2010)

Bucle balanceador:

Bucle 2: Ataques - Flujo de alertas de seguridad - Alertas de seguridad - Alertas remediadas - Probabilidad de ataques - Ataques

En la Figura 18, podemos apreciar el bucle balanceador de color fucsia, además en el bucle anterior se explicó que a mayor cantidad de ataques generan mayor flujo de alertas de seguridad y esta mayor cantidad de alertas de seguridad, que pueden ser remediadas, si son remediadas reducen la probabilidad de que se dé un ataque, entonces hay menor cantidad de ataques.

Bucle balanceador: 

Alertas de seguridad - Alertas remediadas - Alertas de seguridad

En la Figura 18, podemos observar el bucle reforzador negro, en el cual notamos que a mayor cantidad de alertas de seguridad aumentan la cantidad de alertas remediadas (se asume que se tiene mecanismos para remediar una alerta) y a mayor cantidad de alertas remediadas reducen las alertas de seguridad.

Bucle balanceador: 

Total de ataques - Ataques mitigados - Total de ataques

En el bucle balanceador de color morado en la Figura 18, podemos observar que a mayor cantidad de ataques se incrementan los ataques mitigados por los controles de los dispositivos, estos ataques mitigados reducen el total de ataques que tiene la organización, mas no el flujo de ataques, ya que los ataques se mitigan con controles, entonces para la cantidad de ataques que no han sido mitigados, se va a planificar controles (planificación del cumplimiento de políticas).

Bucle reforzador: 

Ataques - Total de ataques - Planificación del cumplimiento de políticas - Control - Vulnerabilidades - Flujo de alertas de seguridad - Alertas de seguridad - Probabilidad de ataque - Ataques

En el bucle reforzador de color azul en la Figura 18, vemos que los ataques incrementan el total de ataques y para los que no han sido mitigados se realiza la planificación del cumplimiento de políticas, esta planificación incrementa el control; pero que pasa si hay incumplimiento de los controles, entonces se incrementan las vulnerabilidades y a mayor cantidad de vulnerabilidades se tiene mayor flujo de alertas de seguridad, que incrementa la cantidad de alertas de seguridad y si no han sido remediadas hay mayor probabilidad de que ocurra un ataque y esto incrementa los ataques.

Bucle balanceador: 

Ataques - Total de ataques - Planificación del cumplimiento de políticas - Control - Vulnerabilidades - Flujo de alertas de seguridad - Alertas de seguridad - Alertas remedidas - Probabilidad de ataque - Ataques

En la Figura 18 se puede observar en el bucle balanceador de color azul la relación que se mencionó anteriormente del flujo de ataques que incrementa el total de ataques, estos incrementan la planificación de cumplimiento de políticas que a su vez aumentan el control; pero si hay incumplimiento de los controles entonces hay más vulnerabilidades y a mayor cantidad de vulnerabilidades se tiene mayor cantidad de alertas de seguridad, estas a su vez aumentan la cantidad de alertas remediadas y a mayor cantidad de alertas remedidas reducen la probabilidad de que ocurra un ataque y esto disminuye la cantidad de ataques.

Bucle reforzador:

Planificación del cumplimiento de políticas - Control-Vulnerabilidades - Flujo de alertas de seguridad - Alertas de seguridad - Planificación del cumplimiento de políticas

En el bucle anterior se vio que a mayor planificación de cumplimento de políticas se incrementa el control; pero si hay incumplimiento de los controles entonces incrementan las vulnerabilidades y a mayor cantidad de vulnerabilidades se tiene mayor cantidad de alertas de seguridad que si no son remediadas es porque los controles tienen vulnerabilidades que conducen a la planificación del cumplimiento de políticas.

Bucle balanceador:

Vulnerabilidades - Vulnerabilidades mitigadas – Vulnerabilidades

Las vulnerabilidades incrementan las vulnerabilidades mitigadas estas vulnerabilidades mitigadas se ven influenciadas por el nivel de capacidad que nos ayuda a mitigar las vulnerabilidades, tomando en cuenta que para la presente tesis resulta importante la seguridad de la empresa (a mayor nivel de capacidad tengo menos vulnerabilidades).

En la Figura 19 se puede apreciar que las vulnerabilidades propician más alertas de seguridad y si actuamos de una manera preventiva con controles entonces tenemos más vulnerabilidades mitigadas.

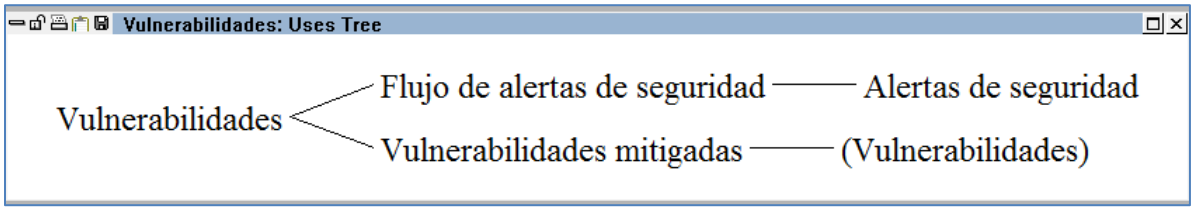


Figura 19. Influencia de las vulnerabilidades.

En la Figura 20 se puede apreciar que aquellos ataques que llegan afectar nuestra organización, es decir si nuestros equipos no estuvieron configurados correctamente o no lo detectaron, conducen a la planificación de nuevas políticas en la organización de manera que nuestro sistema de seguridad actúe de una forma resiliente para la siguiente vez, en cambio si nuestros equipos actuaron correctamente protegiendo nuestra infraestructura, por ciertos patrones, los ataques van a ser mitigados cuando apenas lo detecte.

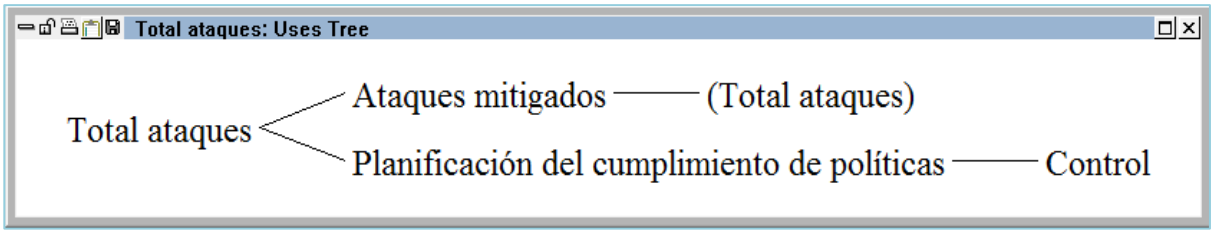


Figura 20. Influencia de ataques.

En la Figura 21 se toma en cuenta un aspecto muy importante del BMIS, sabemos los ataques conducen a las alertas de seguridad en los equipos y esto hace más vulnerable la empresa, entonces "A higher number of vulnerabilities obviously leads to an increased attractiveness of an attack-as does the lack of monitoring or countermeasures. Once it is known that the enterprise is vulnerable from within, this may change the overall attractiveness as a target, and the overall probability of an attack will increase." [Un mayor número de vulnerabilidades obviamente conduce a un mayor atractivo de un ataque, al igual que la falta de monitoreo o contramedidas. Una vez que se sabe que la empresa es vulnerable desde adentro, esto puede cambie el atractivo general como objetivo y aumentará la probabilidad general de un ataque.] (ISACA, 2010, p. 63), por ello existe mayor probabilidad de ataque. Si tengo alertas de seguridad que no han sido remediadas, estas conducen a la planificación del cumplimiento de políticas, a su vez si tengo más

alertas y actuamos preventivamente estas serán remediadas. Las alertas remediadas reducen las alertas de seguridad e influyen en la probabilidad de ataque.

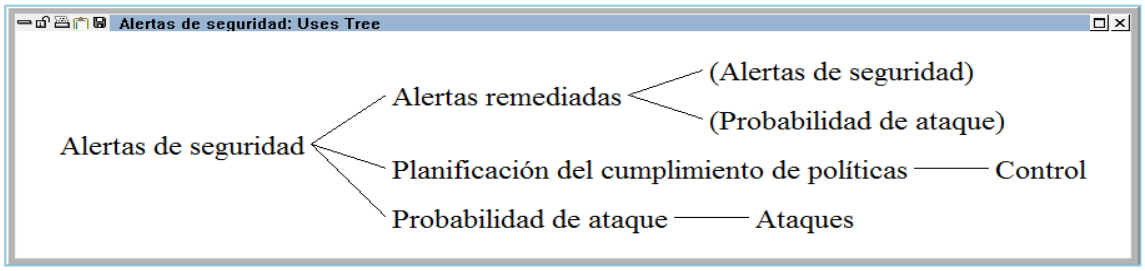


Figura 21. Influencia de las alertas de seguridad.

La NTP-ISO/IEC 27001(2014), define catorce dominios, para la presente tesis se va considerar el dominio de Seguridad de las Comunicaciones. El indicador de cumplimiento de control está basado en los controles de este dominio.

En la Tabla 11 podemos apreciar un esquema de valoración para proceder a valorar controles del dominio.

Tabla 11. Tabla de valoración de la ISO 27001 referente a la 27002.

NO (0%- 30%): El control no se encuentra implantado, o su nivel de implantación y gestión es muy débil. (0)
PARCIAL (40% - 70%): Se tienen algún nivel de implantación con relación a los controles que el dominio específico, pero no se hace en su totalidad. (1)
SI (80% - 100%): El dominio se encuentra implantado. (2)

Fuente: Diagnóstico De Seguridad - Gap Analysis.

En la Tabla 12 apreciamos los controles, los cuales serán evaluados para la corrida del modelo, acorde a la Tabla 11, es clave para determinar la tasa de cumplimiento del control y por

ende la de incumplimiento del control. Se toma en consideración el dominio de Seguridad de las Comunicaciones de la ISO 27001.

Tabla 12**.** Tabla de evaluación de controles acorde al dominio de Seguridad de las Comunicaciones de la ISO 27001 referente a la 27002. Gap Analysis

	Tipo	Control	Premisa	Acción
Controles en la red	mantenimiento	**Controles en la red**	¿La red está adecuadamente administrada y controlada, con el fin de protegerla de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usa la red, incluida la información en tránsito?	Manteniendo a los sistemas y aplicaciones
	mantenimiento	**Seguridad de servicios de red**	¿Las características de seguridad, los niveles de servicio, y los requerimientos de administración de todos los servicios de red, están identificados e incluidos en los acuerdos con los diferentes proveedores de servicios de red, bien sean internos o externos?	Revisión a los acuerdos de los servicios de red.
	mantenimiento	**Segregación en redes**	¿Los controles para segregar grupos de dispositivos de información, usuarios y sistemas de información son adecuados?	Mantenimiento de grupos de dispositivos de información, usuarios y sistemas de información.
Transferencia de información	política	**Políticas y procedimientos de transferencia de información**	¿Hay establecida una política formal de intercambio, procedimientos y controles para proteger el intercambio de información a través de los servicios de comunicación?	Revisión de la política de intercambio de información para los servicios de comunicación.
	política	**Acuerdos de transferencia**	¿Se han establecido acuerdos para el intercambio de información y software dentro de la organización y con organizaciones externas?	Revisión de la política de intercambio de información y software.
	mantenimiento	**Mensajería electrónica**	¿Está adecuadamente protegida la información involucrada en la mensajería electrónica?	Revisión de la seguridad en a la mensajería electrónica.
	política	**Acuerdos de confidencialidad y no revelación**	¿Los acuerdos de confidencialidad y no revelación reflejan las necesidades de la organización, se documentan y revisan?	Revisión de los acuerdos de confidencialidad.

A continuación, en la Tabla 13 se presenta la valoración de la variable nivel de capacidad utilizada en el presente modelo, está basada en los niveles de capacidad del Cobit 5, a su vez puede ser adaptada con los niveles de madurez del Cobit 2019, puesto que maneja el mismo rango de niveles, un nivel de capacidad 1 indica un 20 % para el modelo.

Tabla 13**.** Tabla de valoración del nivel de Capacidad de Cobit 5.

	NIVEL DE CAPACIDAD- Cobit5					
Nivel	0	1	2	3	4	5
Porcentaje	0	0.2	0.4	0.6	0.8	1.00

4.5 Modelado cuantitativo

Ahora una vez descrito nuestro modelo causal, como siguiente paso de la metodología pasaremos a desarrollar el modelo dinámico, con el diagrama de Forrester.

En la Figura 22 podemos apreciar que el total de ataques, las vulnerabilidades y las alertas de seguridad, son las variables de nivel, desde las cuales se puede obtener su comportamiento en el tiempo, de acuerdo con las corridas de los escenarios presentados.

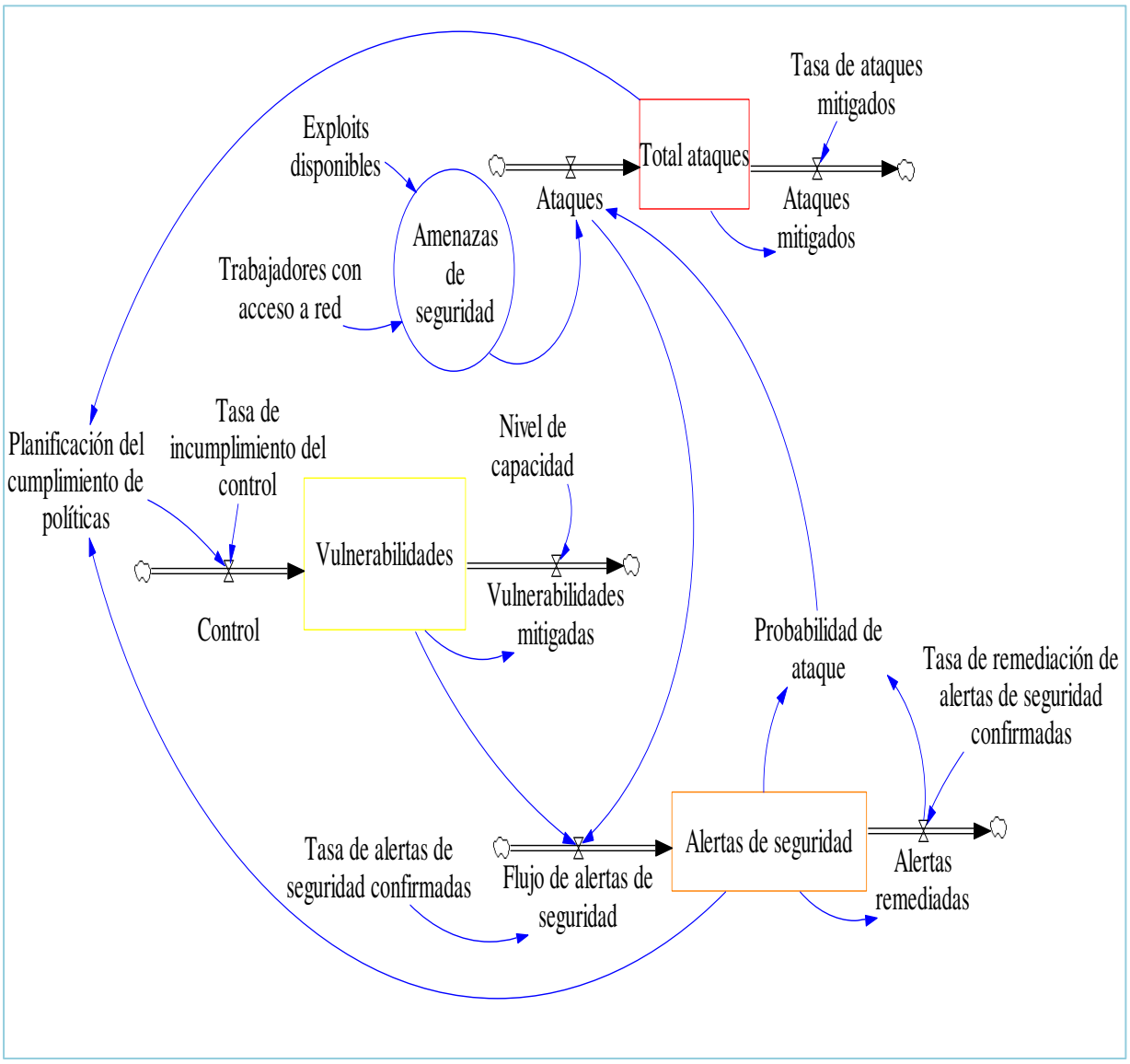


Figura 22. Modelo dinámico para la gestión de seguridad. (Diagrama de Forrester)

A continuación, se detalla las variables y sus unidades de medida respectivas utilizadas en el modelo (Tabla 14) con un nemotécnico que será utilizado para las ecuaciones matemáticas que posee el modelo, presentes en la Tabla 15.

Tabla 14. Variables del modelo cuantitativo.

Tipo de variable	Variable	Unidad de medida	Nemotécnico
Nivel	Vulnerabilidades	número	**VN**
	Total de ataques	número	**TA**
	Alertas de Seguridad	número	**ALE**
Flujo	Control	número/mes	**C**
	Vulnerabilidades mitigadas	número/mes	**VM**
	Ataques	número/mes	**A**
	Ataques mitigados	número/mes	**AM**
	Flujo de alertas de seguridad	número/mes	**FA**
	Alertas remediadas	número/mes	**AR**
Auxiliares	Nivel de capacidad	/mes	**NC**
	Probabilidad de ataque	/mes	**PA**
	Tasa de ataques mitigados	/mes	**TAM**
	Planificación del cumplimiento de políticas	número	**TC**
	Tasa de incumplimiento del control	/mes	**IC**
	Tasa de alertas de seguridad confirmadas	/mes	**AC**
	Tasa de remediación de alertas de seguridad confirmadas	/mes	**TR**
	Trabajadores con acceso a red	número	**NT**
	Exploits disponibles	número	**ED**
	Amenazas de seguridad	número	**AME**

A continuación, se muestra las unidades y fórmulas para el modelo de Vensim.

Para las variables de nivel se tiene:

$$N(t + \Delta t) = N(t) + \Delta t(Fe - Fs)$$

$$N(t) = 0$$

$$\Delta t = mes$$

$$N(t + \Delta t) = 0 + mes\left(\frac{\text{número}}{\text{mes}} - \frac{\text{número}}{\text{mes}}\right) = número$$

(01) Vulnerabilidades= C-VM =INTEG (Control-Vulnerabilidades mitigadas,0),0)

Units: Número de Vulnerabilidades

(02) Total ataques= A-AM= Ataques-Ataques mitigados

Units: Número de ataques

(03) Alertas de seguridad= FA-AR= INTEG (Flujo de alertas de seguridad-Alertas remediadas, 0)

Units: Número de alertas

Para las variables de flujo no influenciadas por una de nivel se tiene:

$$F(t) = M(t)T_n$$

$$F(t) = número\left(\frac{1}{\text{mes}}\right) = \frac{\text{número}}{\text{mes}}$$

(04) Control=TC*IC= Planificación del cumplimiento de políticas*Tasa de incumplimiento del control

Units: Número/Month

(05) Ataques= AME*PA =Amenazas de seguridad*Probabilidad de ataque

Units: Número/Month

Para las variables de flujo influenciadas por una de nivel se tiene:

$$F(t) = X(t)T_n$$

$$F(t) = número\left(\frac{1}{\text{mes}}\right) = \frac{\text{número}}{\text{mes}}$$

(06) Vulnerabilidades mitigadas= VN*NC =Vulnerabilidades*Nivel de capacidad

Units: Número/Month

(07) Alertas remediadas= ALE * TR =Alertas de seguridad*Tasa de remediación de alertas de seguridad confirmadas

Units: Número/Month

(08) Ataques mitigados= TA* TAM= Total ataques *Tasa de ataques mitigados

Units: Número/Month

(09) Flujo de alertas de seguridad=(AC*VN) + A =(Tasa de alertas de seguridad confirmadas*Vulnerabilidades) +Ataques

$$Fx(t) = T_n M(t) + Fy(t)$$

$$F(t) = \left(\frac{1}{\text{mes}}\right) número + \frac{\text{número}}{\text{mes}} = \frac{\text{número}}{\text{mes}}$$

Units: Número/Month

Para las variables auxiliares

(10) Nivel de capacidad = NC = $\left(\frac{1}{\text{mes}}\right)$

Se considera como un equivalente tomado de la Tabla 14 = $(\frac{\text{nivel de capacidad}}{5})$

Units: 1/Month [0,1]

(11) Probabilidad de ataque=1-(AR/AS) = IF THEN ELSE (Alertas remediadas > 0: AND: Alertas remediadas/Alertas de seguridad<=1, 1-(Alertas remediadas/Alertas de seguridad) ,0)

$$\frac{\left(\frac{número}{\text{mes}}\right)}{número} = \frac{1}{\text{mes}}$$

Units: 1/Month [0,1]

(12) Tasa de ataques mitigados=TAM=$\frac{1}{mes}$

$$\frac{Número\ de\ ataques\ a\ la\ red\ interna\ bloqueados\ por\ intrusión}{Número\ de\ ataques\ detectados\ por\ intrusión}$$

Units: 1/Month [0,1]

(13) Planificación del cumplimiento de políticas= ALE+TA=Alertas de seguridad+Total ataques

Número+ Número

Units: Número

(14) Tasa de incumplimiento del control=IC=$\frac{1}{mes}$

Se considera como resultado de la evaluación en la Tabla 13

$$1 - Promedio\ de\ la\ evaluación\ de\ cada\ control$$

$$1 - \frac{\sum Cumplimiento\ de\ cada\ control}{7}$$

Units: 1/Month [0,1]

(15) Tasa de alertas de seguridad confirmadas= AC=$\frac{1}{mes}$

$$\frac{\text{Número de alertas confirmadas}}{\text{Número de alertas generadas}}$$

Units: 1/Month [0,1]

(16) Tasa de remediación de alertas de seguridad confirmadas = TR = $\frac{1}{mes}$

$$\frac{\text{Número de alertas reportadas}}{\text{Número de alertas generadas}}$$

Units: 1/Month [0,1]

(17) Trabajadores con acceso a red = NT= $\frac{1}{mes}$

Units: Número

(18) Exploits disponibles = ED = $\frac{1}{mes}$

Units: Número

(19) Amenazas de seguridad= AME=Trabajadores con acceso a red+Exploits disponibles

Número+ Número

Units: Número

En la Tabla 15 se muestra las fórmulas para cada una de las variables del modelo.

Tabla 15. Fórmulas del modelo cuantitativo.

Descripción de la variable	Fórmula
Vulnerabilidades	**C-VM**
Total de ataques	**A-AM**
Alertas de Seguridad	**FA-AR**
Control	**TC*IC**
Ataques	**AME*PA**
Vulnerabilidades mitigadas	**VN*NC**
Alertas remediadas	**ALE*TR**
Ataques mitigados	**TA *TAM**
Flujo de alertas de seguridad	**(AC*VN) + A**
Nivel de capacidad	**NC** $\equiv (\frac{\text{nivel de capacidad}}{5})$
Probabilidad de ataque	**1-(AR/ALE)**
Tasa de ataques mitigados	**TAM**$\equiv (\frac{Número\ de\ ataques\ a\ la\ red\ interna\ bloqueados\ por\ intrusión}{Número\ de\ ataques\ detectados\ por\ intrusión})$
Planificación del cumplimiento de políticas	**ALE + TA**
Tasa de incumplimiento del control	$\mathbf{IC} \equiv \mathbf{1} - \frac{\sum Cumplimiento\ de\ cada\ control}{7}$
Tasa de alertas de seguridad confirmadas	**AC**$\equiv \frac{\text{Número de alertas confirmadas}}{\text{Número de alertas generadas}}$
Tasa de remediación de alertas de seguridad confirmadas	**TR** $\equiv \frac{\text{Número de alertas reportadas}}{\text{Número de alertas generadas}}$
Trabajadores con acceso a red	**NT**
Exploits disponibles	**ED**
Amenazas de seguridad	**ED + NT**

4.6 Evaluación y análisis del modelo

Para la validación del modelo se ha considerado escenarios de una empresa del sector financiero (Empresa A) en diferentes tiempos, todas evaluadas en un periodo de seis meses, puesto que semestralmente se tienen reportes internacionales publicados, la primera corrida consiste en el caso que el sistema no tenga una adecuada gestión de su seguridad denominada como "Escaso Control", luego se detalla un segundo caso que tenga una adecuada gestión de seguridad, denominada como "Gestión de Seguridad", la tercera corrida está basada en los reportes de la Empresa A denominada como "Empresa A", luego se muestra el resultado de la evaluación de las tres corridas y un escenario estratégico del modelo.

En la Tabla 16 se muestran los valores para el primer escenario llamado "Escaso Control".

Tabla 16. Data para el primer escenario (escaso control)

(Consultada el 02 de agosto de 2019).

Variable (Nemotécnico)	**Unidad de medida**	Valores Iniciales	**Fuente**
VN	número	**121618**	https://www.cvedetails.com/
TA	número	**0**	Caso de la empresa.
ALE	número	**300**	Caso de la empresa.
NC	/mes	**0**	Equivalente al nivel de capacidad 0.
TAM	/mes	$\frac{1}{5}$ **=0.2**	Caso de la empresa.
IC	/mes	**1 − 0.36=0.64**	Caso de la empresa.
AC	/mes	$\frac{72}{300}$ **=0.24**	Cisco (2018).
TR	/mes	$\frac{129}{300}$ **=0.43**	Cisco (2018).
NT	número	**600**	Caso de la empresa.
ED	número	**5**	https://www.exploit-db.com Infraestructura

Para la determinación del cumplimiento del control en el primer escenario, se ha establecido bajo las preguntas tomadas de la Tabla 12. En la Tabla 17 podemos observar los resultados obtenidos sobre las acciones tomadas para este primer escenario descuidado, se obtiene un nivel de cumplimiento promedio de 36 % por lo tanto el incumplimiento toma el valor de 64%.

Tabla 17. Evaluación del cumplimiento del control para el primer escenario (escaso control).

Cumplimiento	**si**	**parcial**	**no**
Acciones	**(2)**	**(1)**	**(0)**
Manteniendo a los sistemas y aplicaciones.			x
Revisión de los acuerdos de los servicios de red.		x	
Mantenimiento de grupos de dispositivos de información, usuarios y sistemas de información.		x	
Revisión de la política de intercambio de información para los servicios de comunicación.		x	
Revisión de la política de intercambio de información y software.		x	
Revisión de la seguridad en a la mensajería electrónica.			x
Revisión de los acuerdos de confidencialidad.		x	

La Figura 23 corresponde al primer escenario, falta mucho para alcanzar el cumplimiento requerido. La línea de color rojo une los puntos del uno al siete que son los siete controles considerados, cada punto tiene un valor esperado de dos, es decir que cumpla con todos los controles; la línea de color azul muestra cómo se encontraría Empresa A para este caso, vemos que

hay una brecha bastante notoria que separa la gráfica de color rojo y la de color azul, para este caso hay muy poco cumplimiento del control.

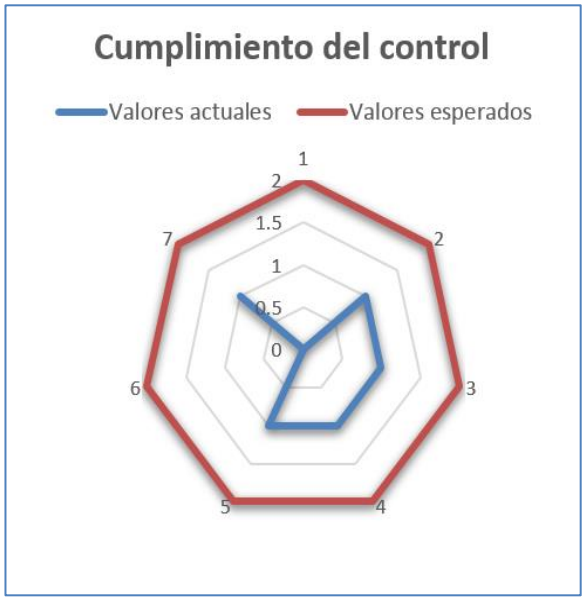


Figura 23. Cumplimiento del control para el primer escenario (escaso control).

En la Figura 24 se muestra el comportamiento del modelo dinámico resultado de correr el primer escenario, a medida de ir actualizando nuestras variables auxiliares, las gráficas van cambiando acorde al escenario, de la Tabla 14 se obtiene un nivel de capacidad cero que quiere decir que los procesos no alcanzan su propósito.

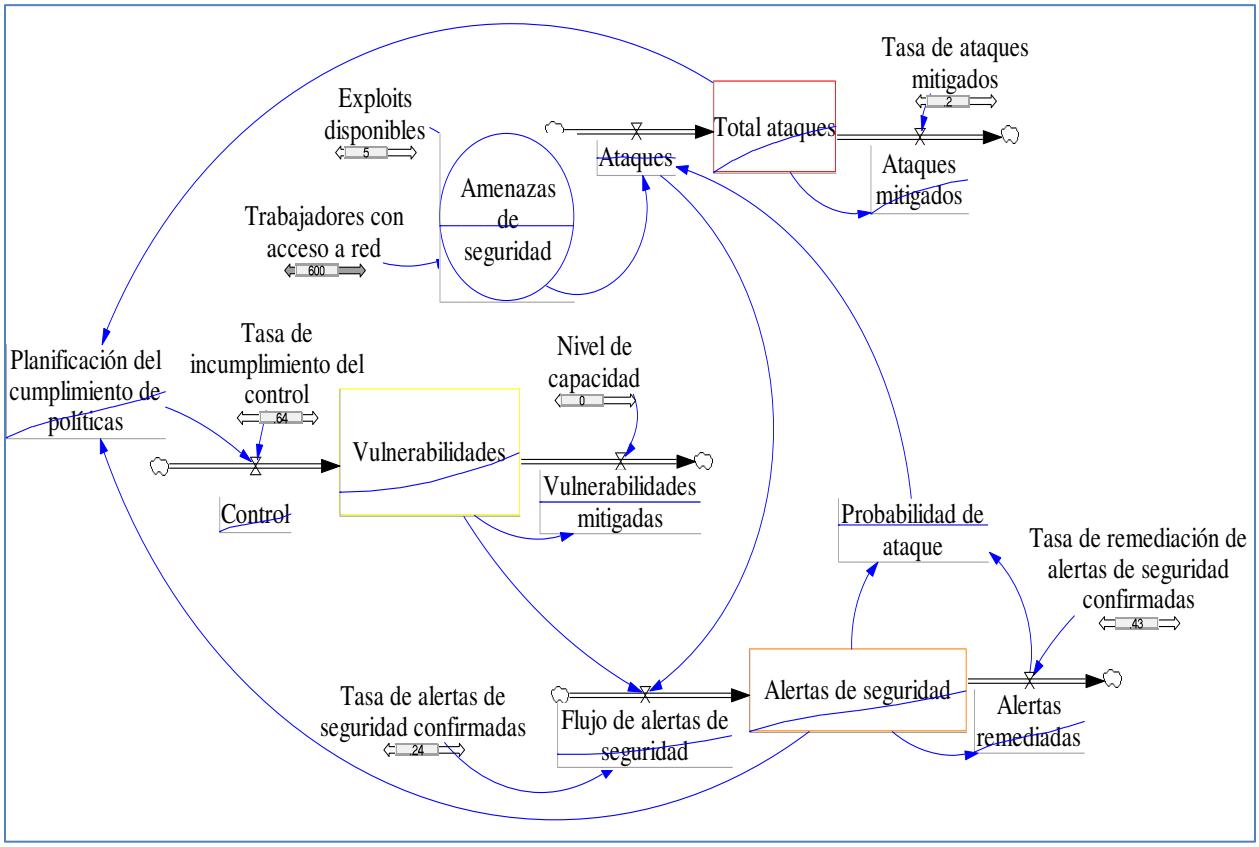


Figura 24. Primera corrida del modelo dinámico para la gestión de seguridad (escaso control).

A continuación en la Figura 25, Figura 26 y Figura 27 corresponden a tres variables de nivel involucradas en el modelo para el escenario "Escaso Control", se observa que a medida que las alertas incrementan existe mayor probabilidad de ser atacados, como inicialmente hay cierta cantidad de vulnerabilidades elevada, entonces hasta el primer mes se mantienen las vulnerabilidades; pero en el transcurso del tiempo si no se realiza algo para seguir protegiendo la infraestructura, las vulnerabilidades van a seguir en ascenso a tal medida de sufrir ataques hacia la infraestructura.

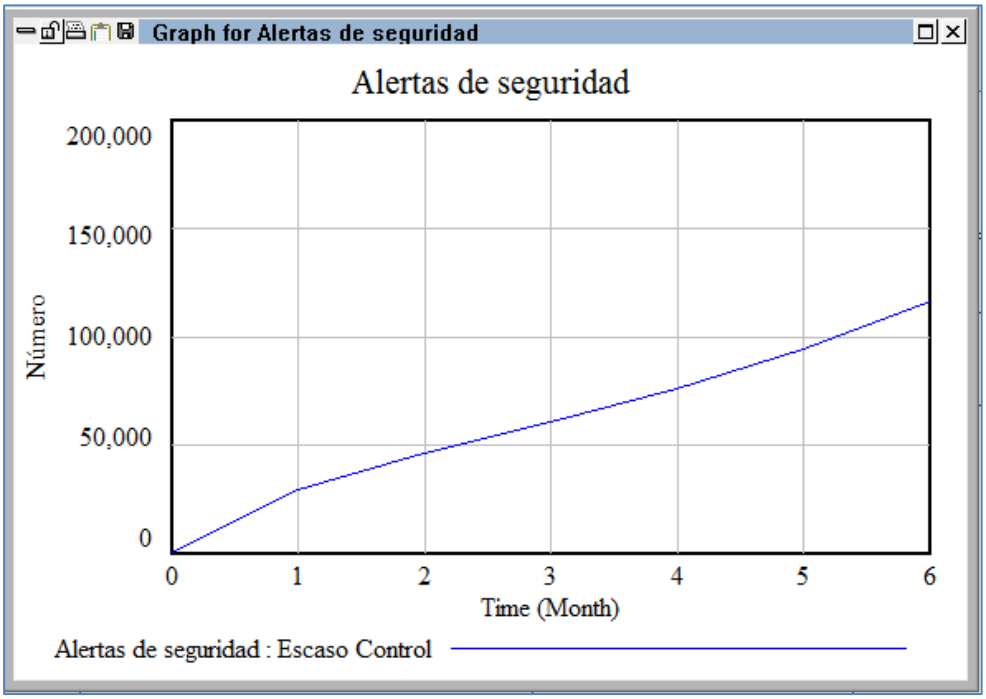


Figura 25. Número de alertas para la primera corrida.

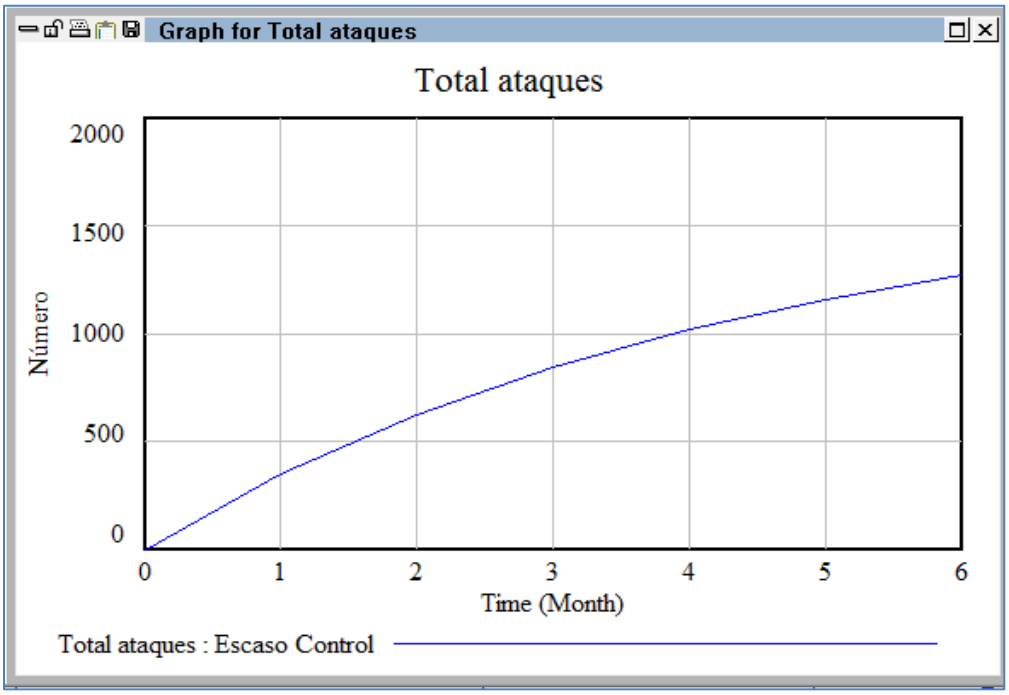


Figura 26. Número de ataques para la primera corrida.

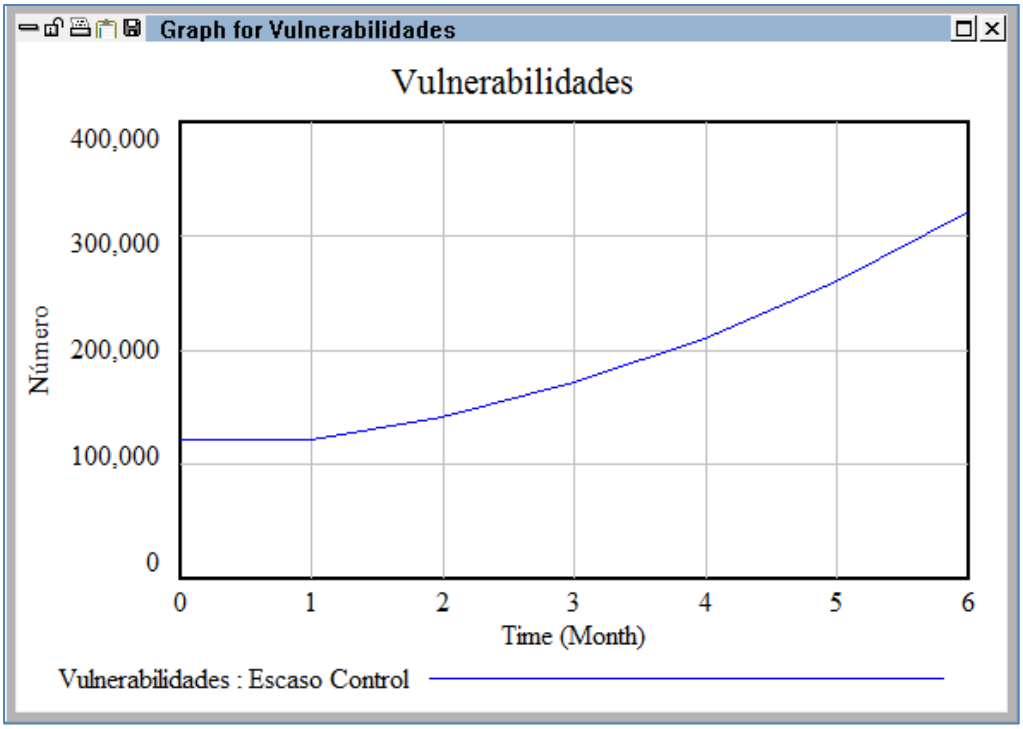


Figura 27. Número de vulnerabilidades para la primera corrida.

En otro caso en que la empresa tiene un mayor porcentaje de incumplimiento del control, las vulnerabilidades tienden a incrementar aún más y las alertas también, el total de ataques se mantiene en aumento, esto es porque los equipos de seguridad están bien configurados para afrontar ataques; la razón por la que no disminuyen y se mantienen es porque no se está cumpliendo las políticas de control y para mitigar ataques se necesita el cumplimiento de controles.

Si se cumple con todos los controles o casi todos los controles, es decir no se tiene controles con vulnerabilidades, estas a lo largo del tiempo establecido de prueba que son seis meses, pueden disminuir casi al punto de llegar a cero, teniendo en cuenta un nivel de capacidad 2 que representa un proceso implementado de forma gestionada que es 40% del cumplimiento, este caso modificado será denominado como "Bastante Control".

En la Figura 28, se puede observar una comparación del comportamiento de las vulnerabilidades entre el primer escenario "Escaso Control" de color azul, con el presente caso

modificado “Bastante Control” de color rojo que representa un mayor control, en el cual disminuyen las vulnerabilidades y se puede identificar el comportamiento de las vulnerabilidades mitigadas como cada vez existe menos vulnerabilidades.

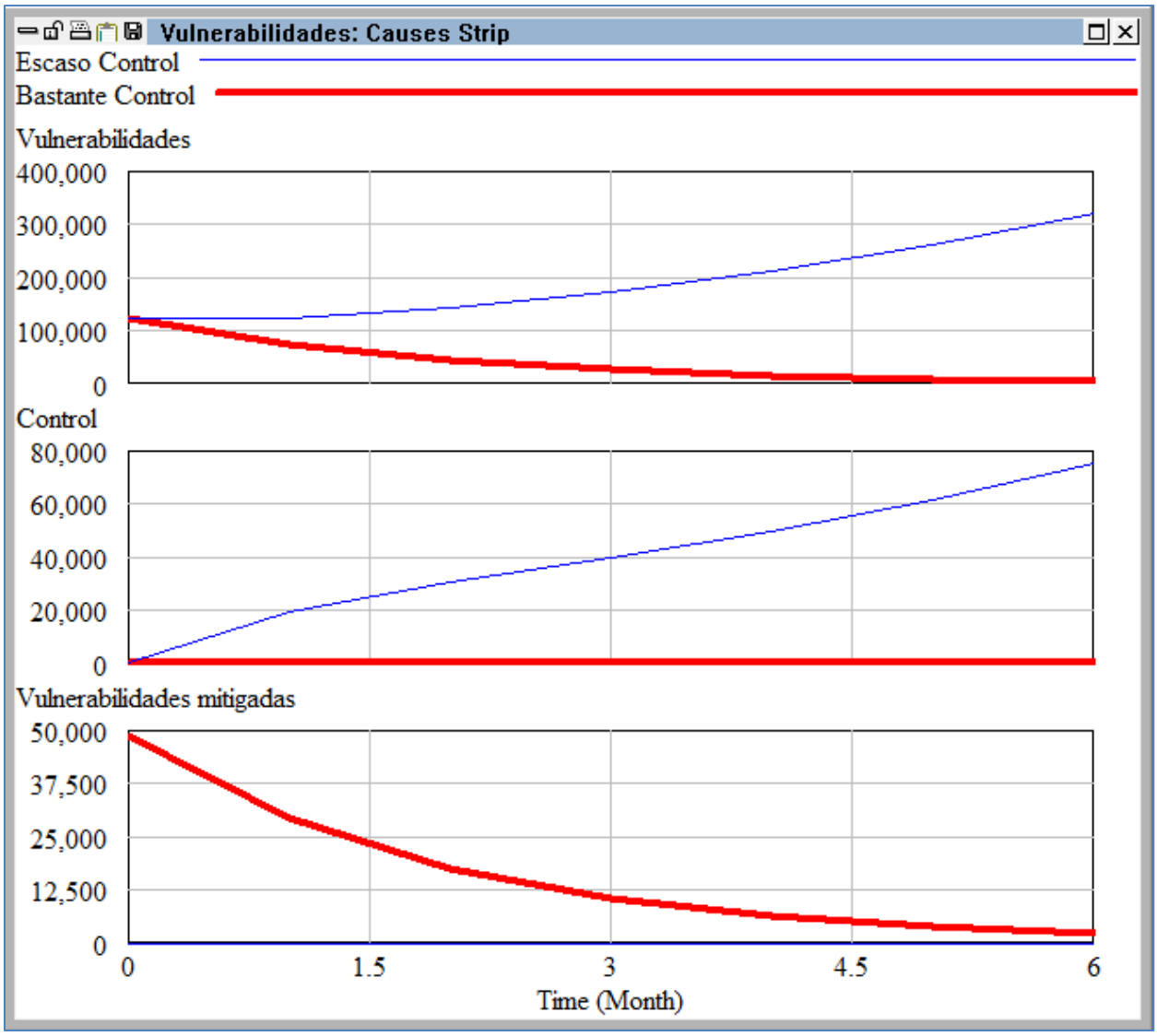


Figura 28. Comparación de los escenarios de vulnerabilidades con escaso control y mayor cumplimiento de control.

La Figura 29 muestra una comparación entre el escenario “Escaso Control” de color azul y la línea de color rojo se puede identificar el comportamiento de las alertas, para este tipo de escenario de “Bastante Control” en el que se cumple con los controles, el flujo de alertas de seguridad van disminuyendo a medida que pasa el tiempo, las alertas de seguridad al igual que las

alertas remediadas todavía se mantienen incremento hasta llegar a un determinado punto de equilibrio en el que empiezan a disminuir, esto sucede porque todavía existe un cierto nivel de alertas que remediar.

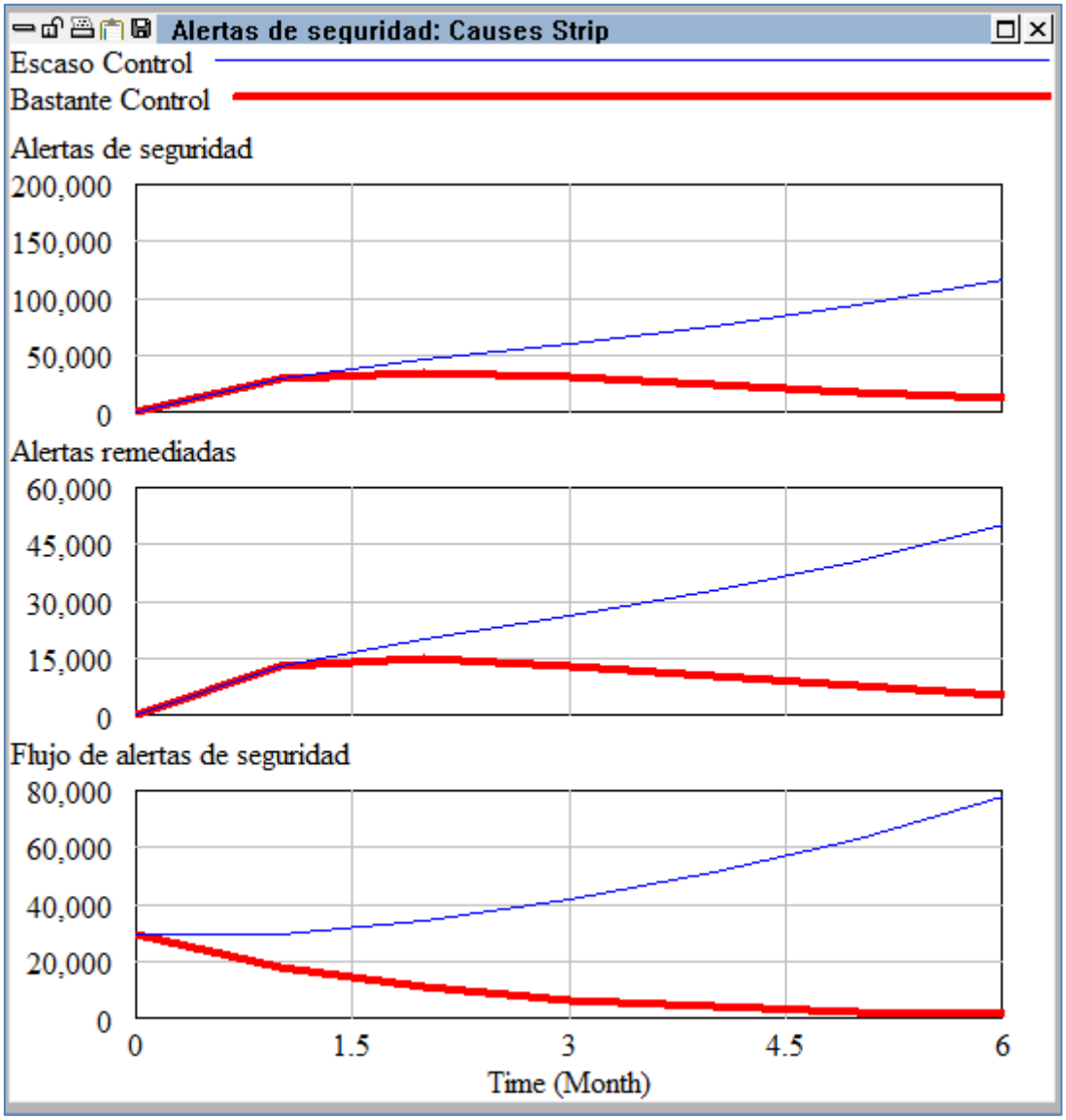


Figura 29. Comparación de los escenarios de alertas con escaso control y mayor cumplimiento de control.

A continuación, un segundo escenario llamado "Gestion de Seguridad".

En la Tabla 18 se muestran los valores para la segunda corrida, es importante resaltar que debemos de cambiar el panorama global de la tasa de remediación de alertas de seguridad

confirmadas, eso depende de cada organización, si no existirá mayor probabilidad a ser atacados, para este escenario se considera 100% el valor de la tasa.

Tabla 18. Data para el segundo escenario (gestión de seguridad)**.**

(Consultada el 02 de agosto de 2019).

Variable (Nemotécnico)	Unidad de medida	Valores Iniciales	Fuente
VN	número	**121618**	https://www.cvedetails.com/
TA	número	**0**	Caso de la empresa.
ALE	número	**300**	Caso de la empresa.
NC	/mes	$\frac{5}{5} = 1$	Equivalente al nivel de capacidad 5.
TAM	/mes	$\frac{99}{100} = 0.99$	Caso de la empresa.
IC	/mes	$1 - 0.93 = 0.07$	Caso de la empresa.
AC	/mes	$\frac{72}{300} = 0.24$	Cisco (2018).
TR	/mes	$\frac{300}{300} = 1$	Caso de la empresa.
NT	número	**600**	Caso de la empresa.
ED	número	**5**	https://www.exploit-db.com Infraestructura

Para la determinación del cumplimiento del control en el segundo escenario "Gestión de Seguridad", se ha establecido bajo las preguntas tomadas de la Tabla 12. En la Tabla 19 se puede observar los resultados obtenidos.

Tabla 19. Evaluación del cumplimiento del control para el segundo escenario (gestión de seguridad).

Cumplimiento	**si**	**parcial**	**no**
Acciones	**(2)**	**(1)**	**(0)**
Manteniendo a los sistemas y aplicaciones.	x		
Revisión de los acuerdos de los servicios de red.	x		
Mantenimiento de grupos de dispositivos de información, usuarios y sistemas de información.	x		
Revisión de la política de intercambio de información para los servicios de comunicación.	x		
Revisión de la política de intercambio de información y software.		x	
Revisión de la seguridad en a la mensajería electrónica.	x		
Revisión de los acuerdos de confidencialidad.	x		

En el gráfico radial de la Figura 30 se observa que, el segundo escenario "GestiónSeguridad", de color azul se aproxima más a los valores esperados de color rojo, por tanto, tiene un alto nivel de cumplimiento, obteniéndose un valor de 93 %, el incumplimiento del control llega a un valor mínimo de 7%.

La Figura 31 muestra la segunda corrida para el modelo (se considera un nivel de capacidad cinco como 100% de su cumplimiento), para un escenario de mayor cumplimiento de controles y respuesta oportuna ante alertas como a pesar de existir exploits podemos actuar de forma resiliente ante ataques y en el transcurso del tiempo vamos teniendo menos vulnerabilidades en los controles.

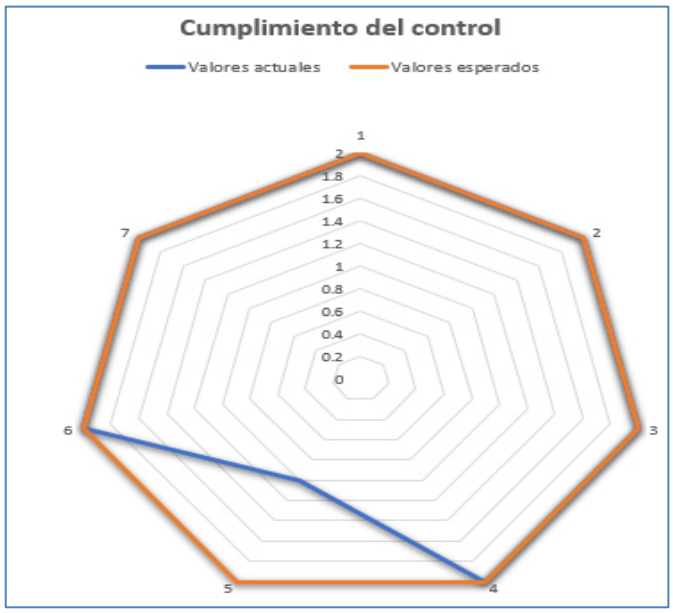


Figura 30. Cumplimiento del control segundo escenario (gestión de seguridad).

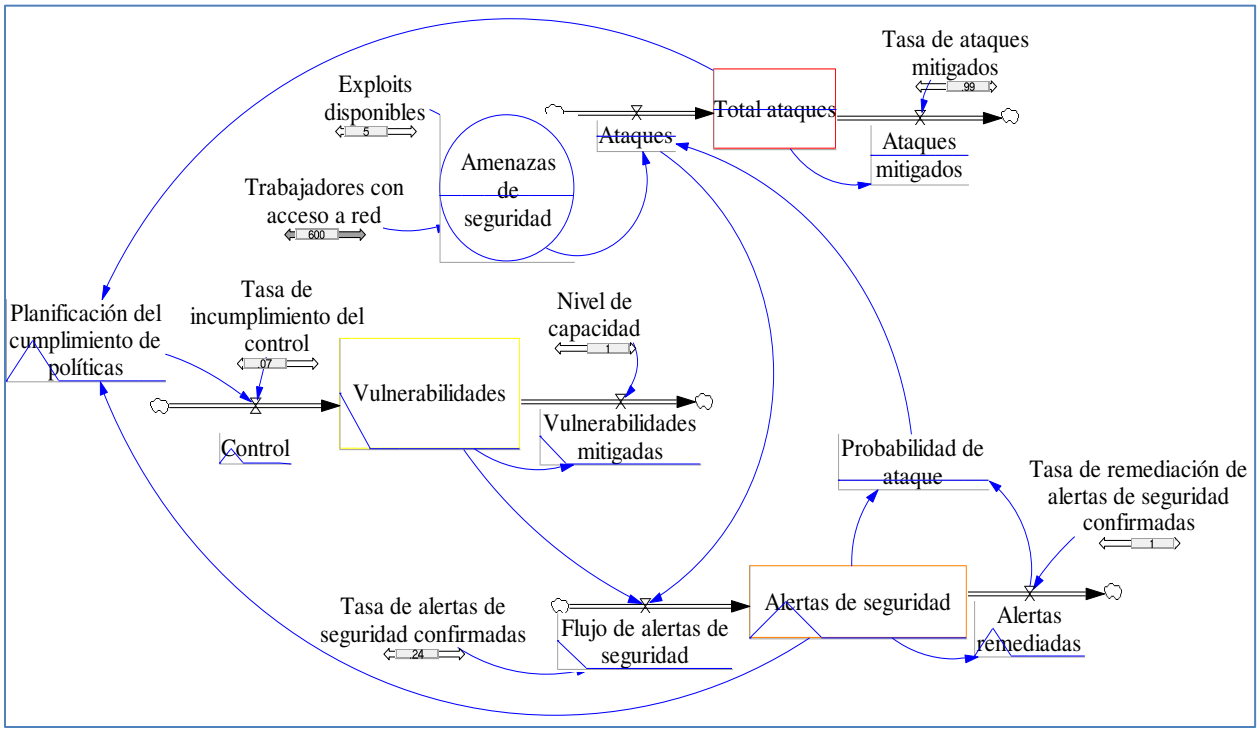


Figura 31. Segundad corrida del modelo dinámico para la gestión de seguridad. (Diagrama de Forrester con seguridad)

En la Figura 32 se evidencia que las vulnerabilidades tienden a decrecer para este segundo escenario de "Gestión de Seguridad", inicialmente se tenía un valor superior a cien mil, durante el primer mes tiende a bajar, luego se estabiliza a casi cero, el valor de los siguientes seis meses va a depender del escenario en el que se encuentre la organización.

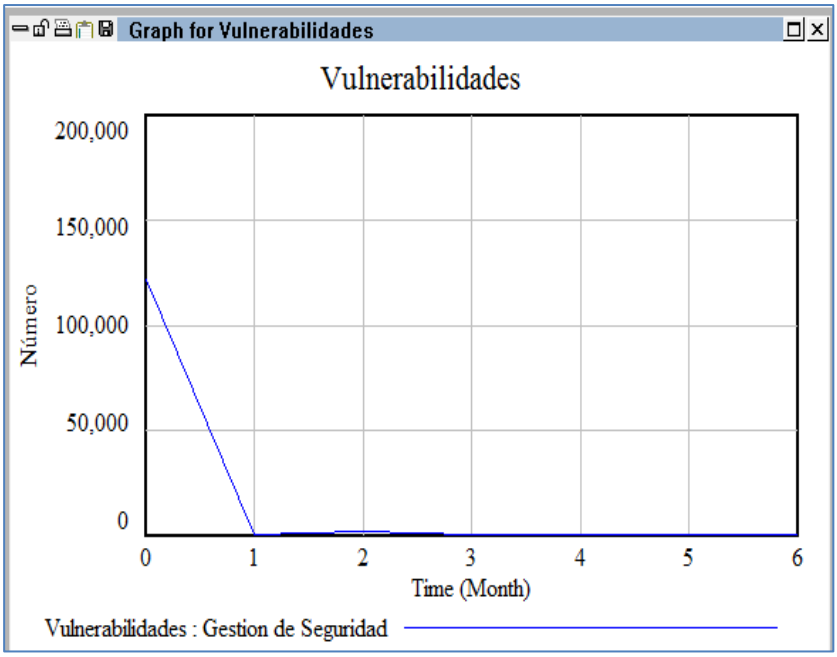


Figura 32. Número de vulnerabilidades para la segunda corrida.

En la Figura 33 se observa que las alertas tienden a incrementar durante el primer mes puesto que existe vulnerabilidades que faltan mitigar, después de ese periodo tiende a bajar, mientras se mantenga el mismo valor de las variables involucradas.

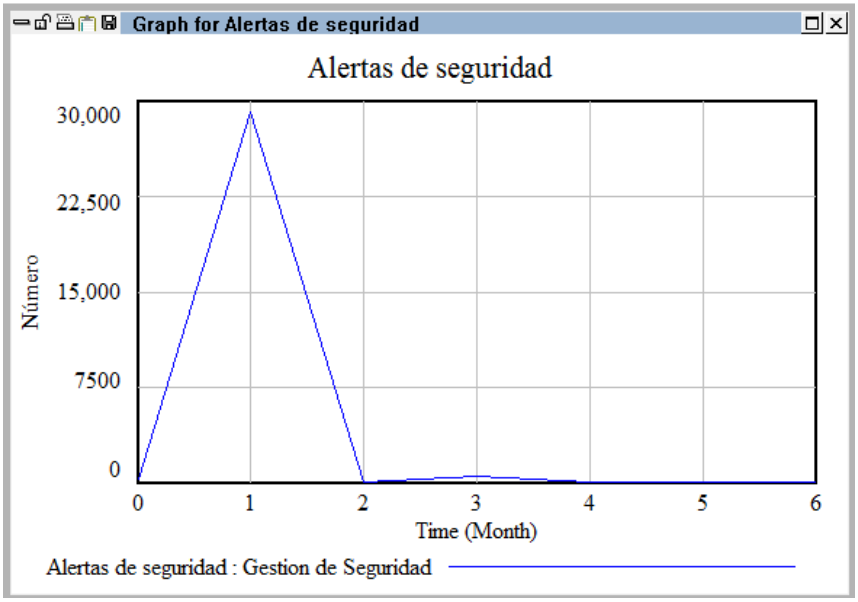


Figura 33. Número de alertas para la segunda corrida.

La Figura 34 muestra que el número de ataque es cero puesto que tenemos remedidas todas las alertas, esto quiere decir que la organización está preparada ante un posible ataque.

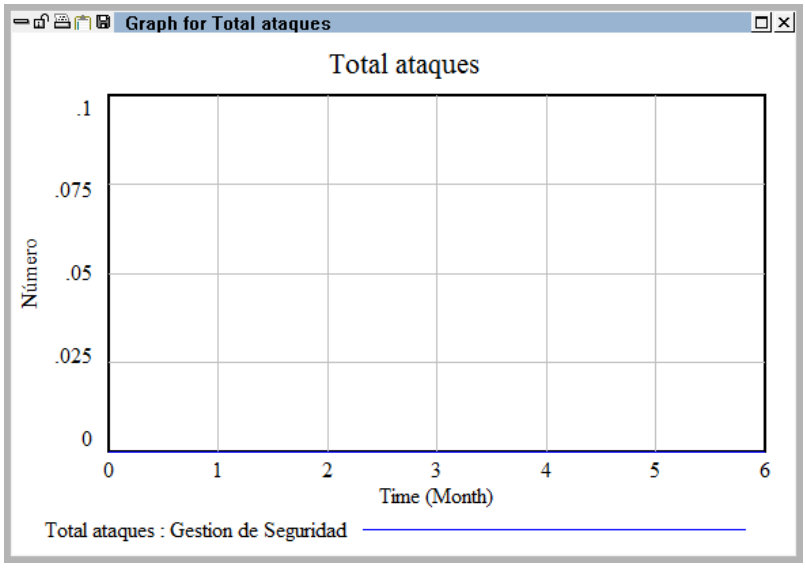


Figura 34. Número de ataques para la segunda corrida.

En la Figura 35 se observa los valores que se le han asignado al modelo para ambas corridas, en el primer caso de "Escaso Control" con un nivel de capacidad cero y para el segundo caso de "Gestión de Seguridad" con un nivel de capacidad cinco; en relación a los ataques mitigados en el primer caso al empresa mitiga solo el 2 % de ataques, mientras que el segundo caso casi todos con un 99%, el resto que no es mitigado pasa como alerta para ser remediado; la tasa de incumplimiento del control para el primer caso es bastante alta con un 64 %, en el segundo caso cumple casi todos los controles al 93%; la tasa de remedición de alertas de seguridad que no son por falsos dispositivos en el segundo caso remedian todo a diferencia del primer caso que es el panorama actual según el reporte de Cisco, en el que se ve la deficiencia en este aspecto por parte de las organizaciones.

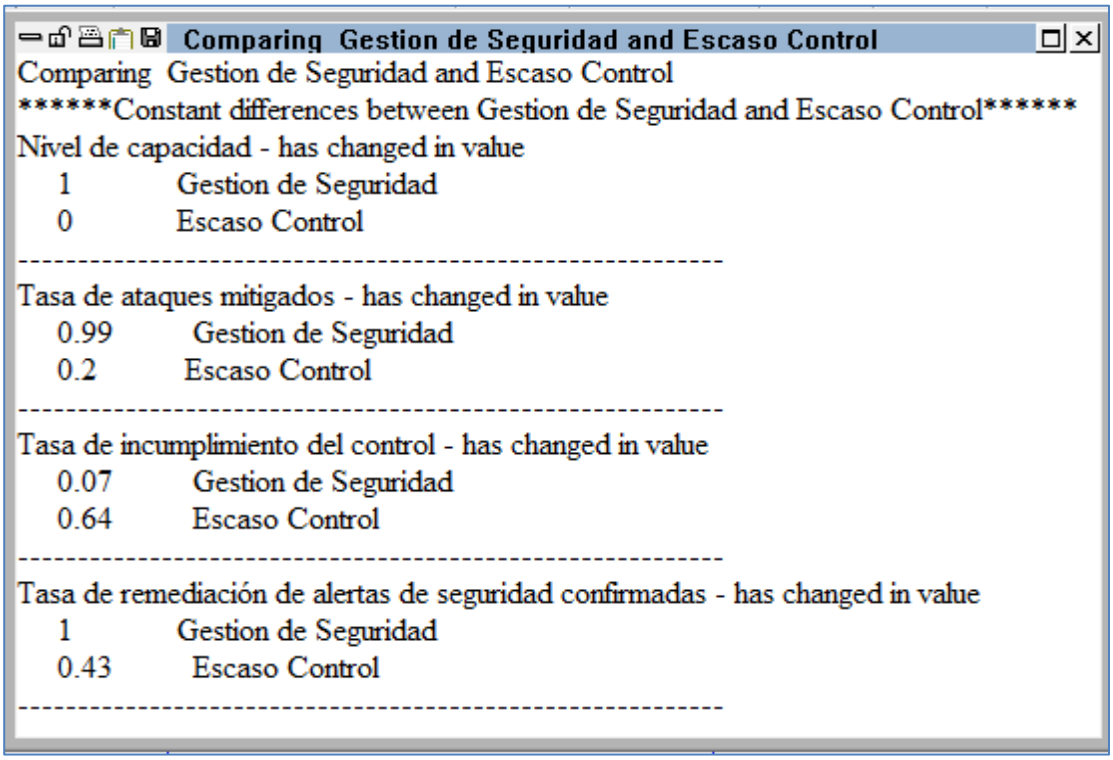


Figura 35. Comparación de datos ambas corridas (escaso control y gestión de seguridad).

La Figura 36 muestra las corridas de ambos escenarios "Escaso Control" y "Gestión de Seguridad", en el primer caso de color rojo, a medida que incrementan las vulnerabilidades, incrementa el total de ataques y las alertas de seguridad; el segundo caso de color azul caso se observa que a medida que las vulnerabilidades decrecen, las alertas disminuyen y los ataques se mantienen en cero.

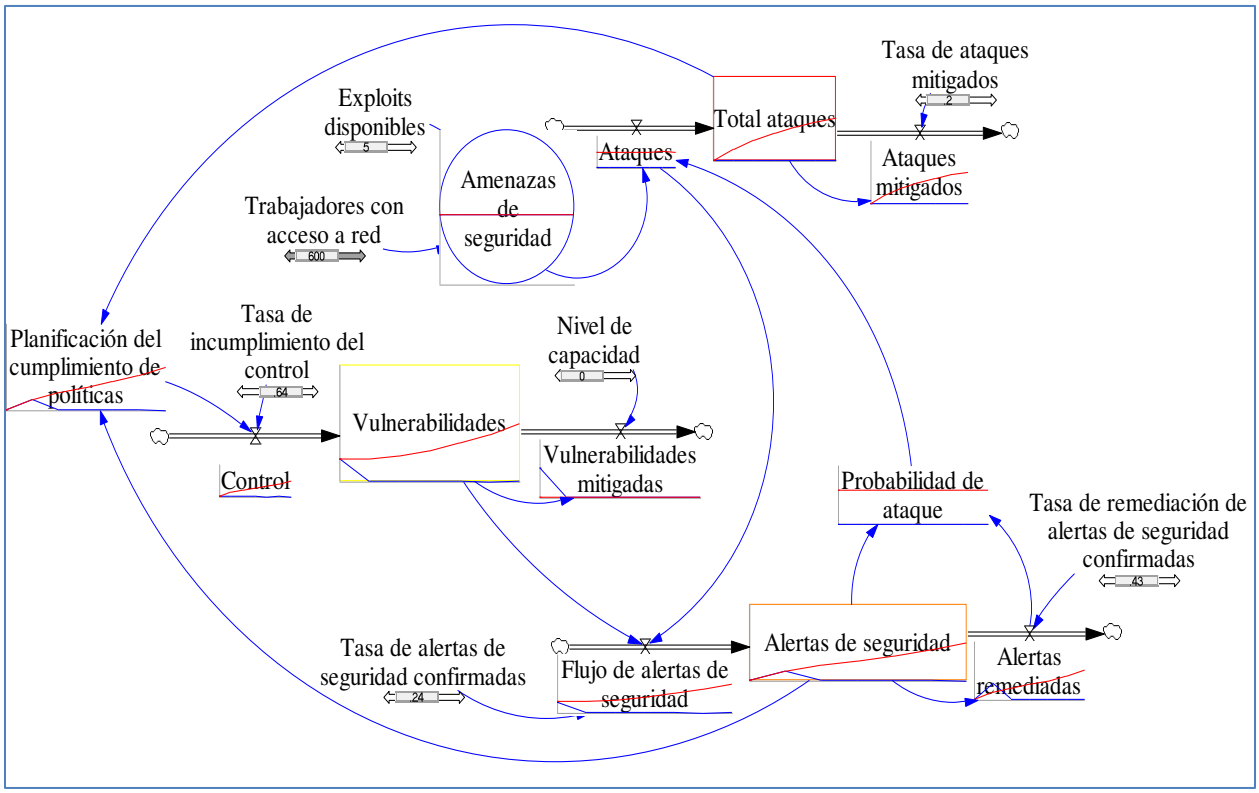


Figura 36. Comparación de ambas corridas (escaso control y gestión de seguridad).

En la Figura 37 se observa con más detalle el valor del total de ataque para esta segunda corrida llamada "Gestión de Seguridad" que es cero a diferencia de la primera corrida llamada "Escaso Control" que va en aumento.

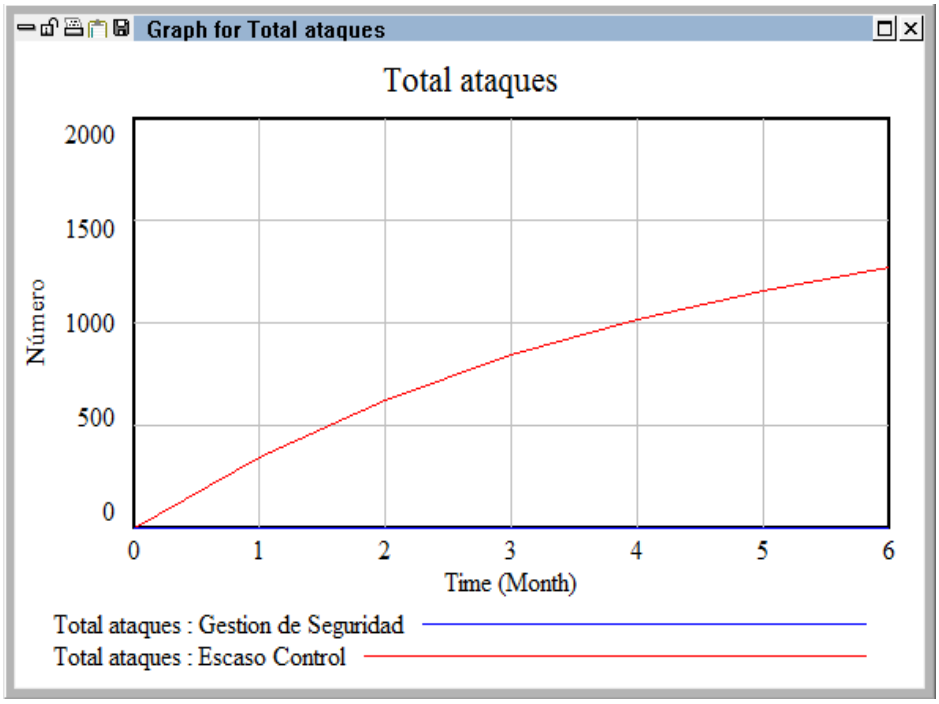


Figura 37. Comparación de ataques en ambas corridas (escaso control y gestión de seguridad).

En la Figuras 38 y Figura 39 se evidencia la disminución de las alertas y vulnerabilidades de la segunda corrida con relación a la primera corrida.

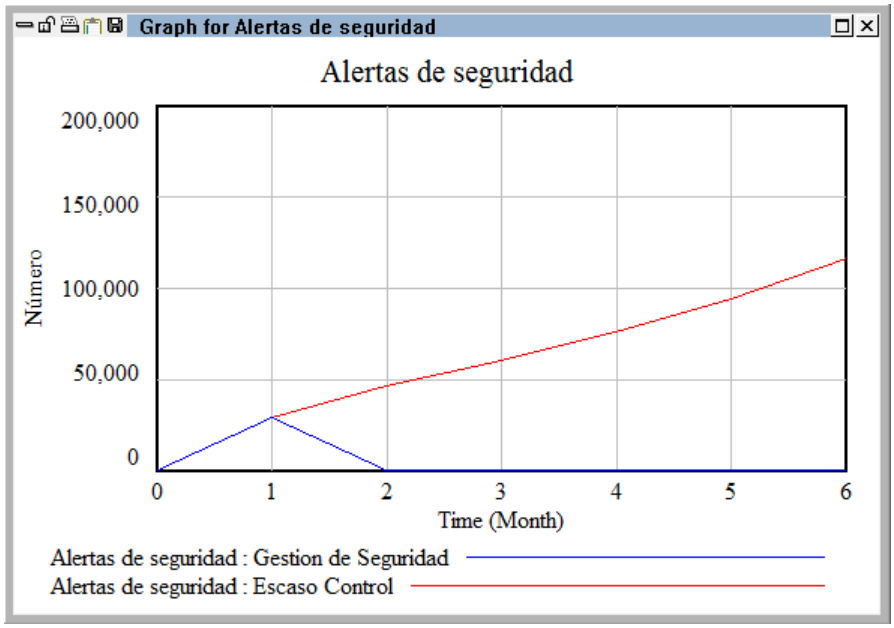


Figura 38. Comparación de alertas de seguridad en ambas corridas (escaso control y gestión de seguridad).

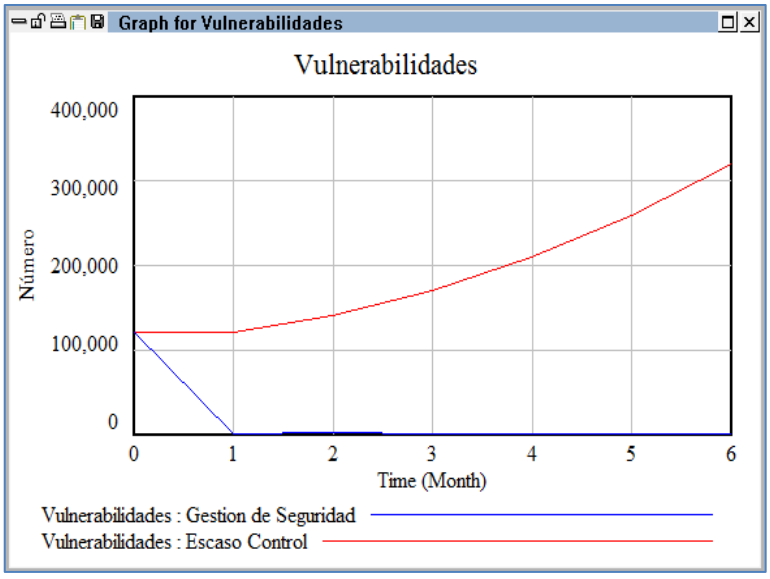


Figura 39. Comparación de vulnerabilidades de seguridad en ambas corridas (escaso control y gestión de seguridad).

En la Figura 40 se puede identificar que en la segunda corrida hay menor planificación de políticas generadas por vulnerabilidad o ataques a diferencia de la primera corrida que si se requiere mayor planificación.

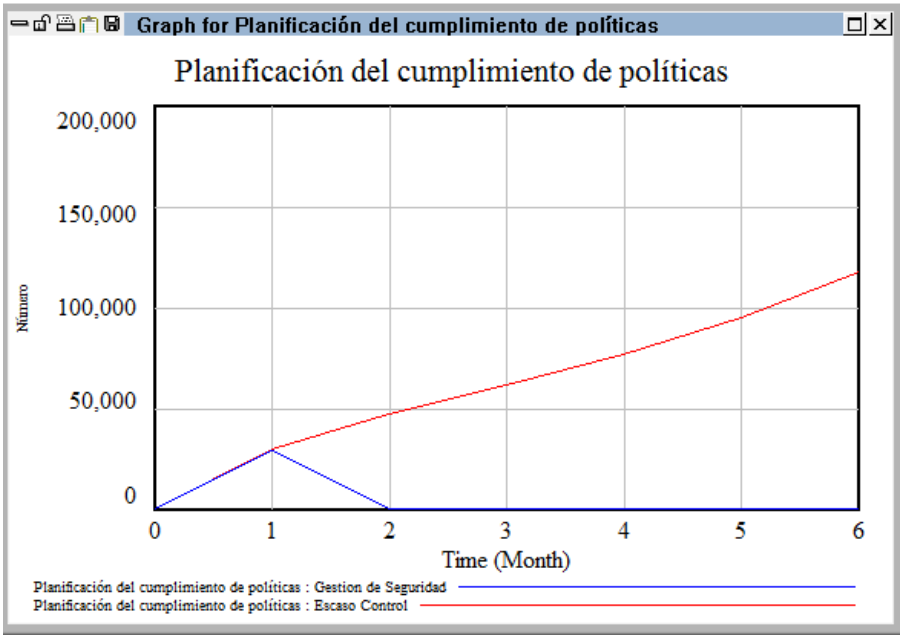


Figura 40. Comparación de la planificación del cumplimiento de políticas de seguridad en ambas corridas (escaso control y gestión de seguridad).

Para tercera corrida de un caso de la "Empresa A", se toma valores iniciales de la Tabla 20 acorde a los reportes que tiene el área de seguridad informática para seguridad de la información y reportes internacionales.

Tabla 20. Evaluación del cumplimiento del control para el tercer escenario (Empresa A).

(Consultada el 02 de agosto de 2019)

Variable (Nemotécnico)	**Unidad de medida**	Valores Iniciales	**Fuente**
VN	número	**121618**	https://www.cvedetails.com/
TA	número	**0**	Caso de la empresa.
ALE	número	**300**	Caso de la empresa.
NC	/mes	$\frac{3}{5}$ **=0.6**	Caso de la empresa.
TAM	/mes	$\frac{50}{100}$ **=0.5**	Caso de la empresa.
IC	/mes	**1 − 0. 7 =0.3**	caso de la empresa.
AC	/mes	$\frac{72}{300}$ **=0.24**	Cisco (2018).
TR	/mes	$\frac{225}{300}$ **=0.75**	Caso de la empresa.
NT	número	**600**	Caso de la empresa.
ED	número	**5**	https://www.exploit-db.com

En la Figura 41 se distingue la corrida para el tercer caso en la línea de color verde, llamado "Empresa A", acorde a la empresa presenta un nivel de capacidad tres que equivale a un 60% de su cumplimiento, en comparación de las dos anteriores, la primera llamada "Escaso Control" es la línea de color rojo y la segunda de color azul llamada "Gestión de Seguridad". La "Empresa A" está en un término medio; más inclinado al de la buena gestión en seguridad.

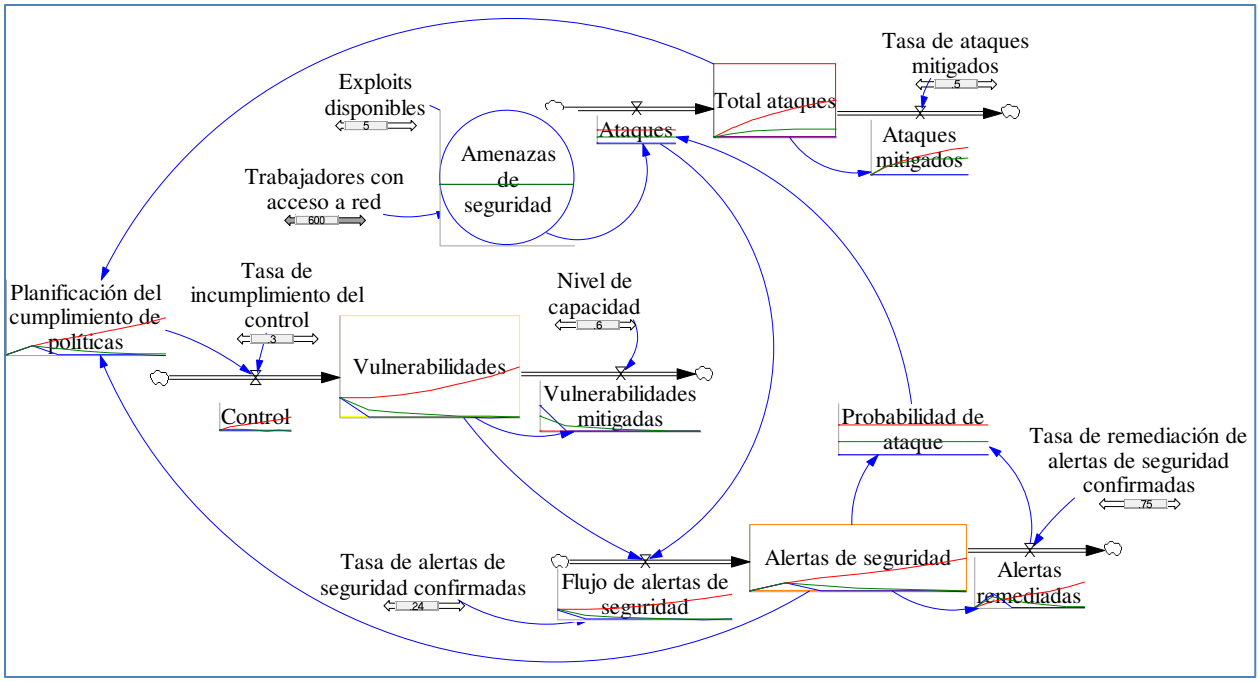


Figura 41. Comparación de las tres corridas.

En la Figura 42 se puede observar que la "Empresa A" está un poco propensa a sufrir ataques, en comparación con los dos escenarios anteriores de "Escaso Control" y "Gestión de Seguridad".

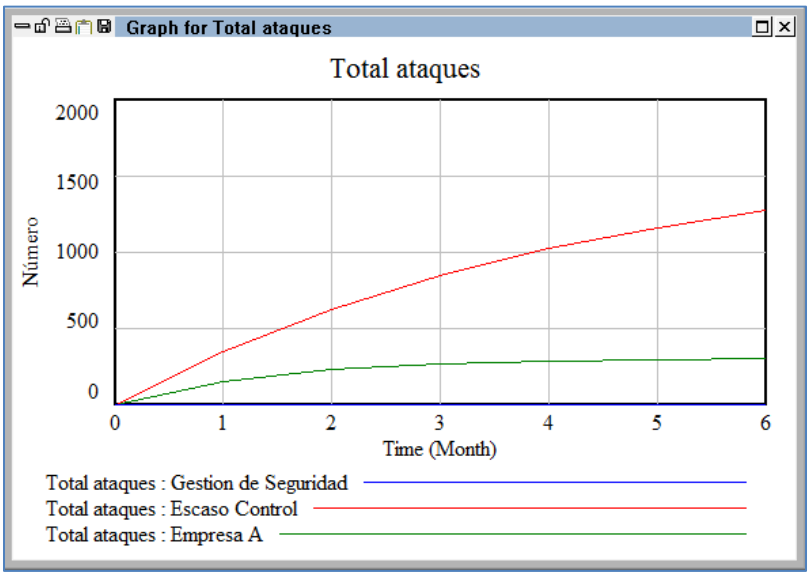


Figura 42. Comparación del total de ataques en la tercera corrida.

En la Figura 43 se puede identificar que las vulnerabilidades tienden a disminuir para el tercer escenario de la "Empresa A"; pero quedan presente vulnerabilidades que, si no se mitigan pronto, se mantendrán, para ello se debe evaluar los controles y tomar medidas para mejorar el cumplimiento de ellos.

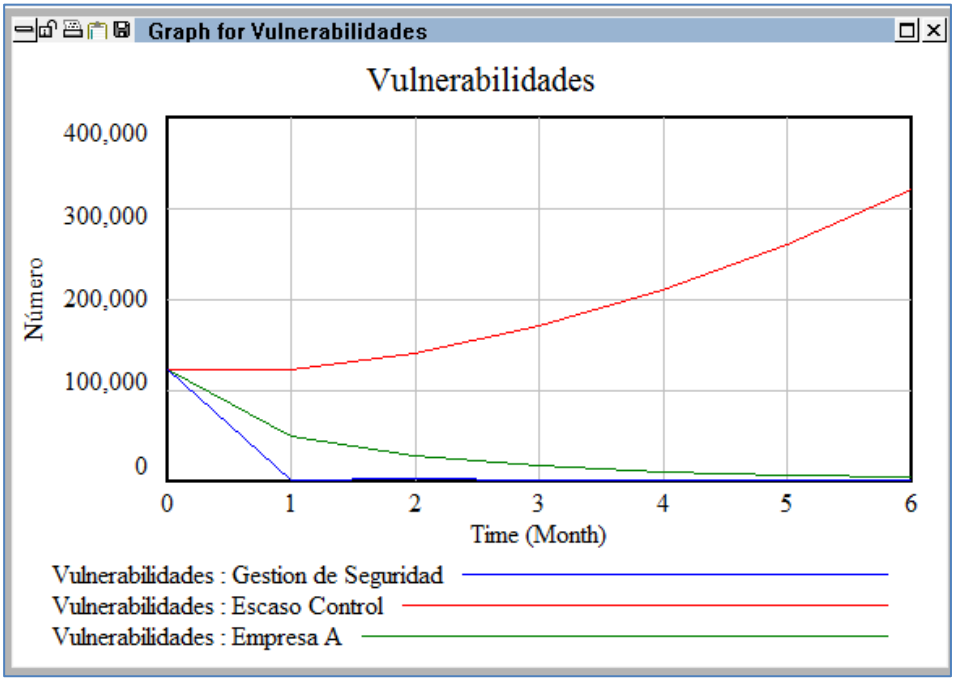


Figura 43. Comparación de las vulnerabilidades en la tercera corrida (Empresa A).

En el escenario "Empresa A" de color verde (Figura 44), vemos que durante el primer mes va a continuar con alertas, luego tiende a disminuir poco, se necesita remediar ello lo más pronto posible para revertir este escenario.

En la Figura 45 se observa que las alertas y vulnerabilidades tienden a disminuir mientras que los ataques están en aumento para la corrida de la "Empresa A" (Figura 46) puesto que no se ha incrementado la tasa de mitigación de ataques y alertas, si se mantiene así hasta el sexto mes, la organización podría sufrir ataques.

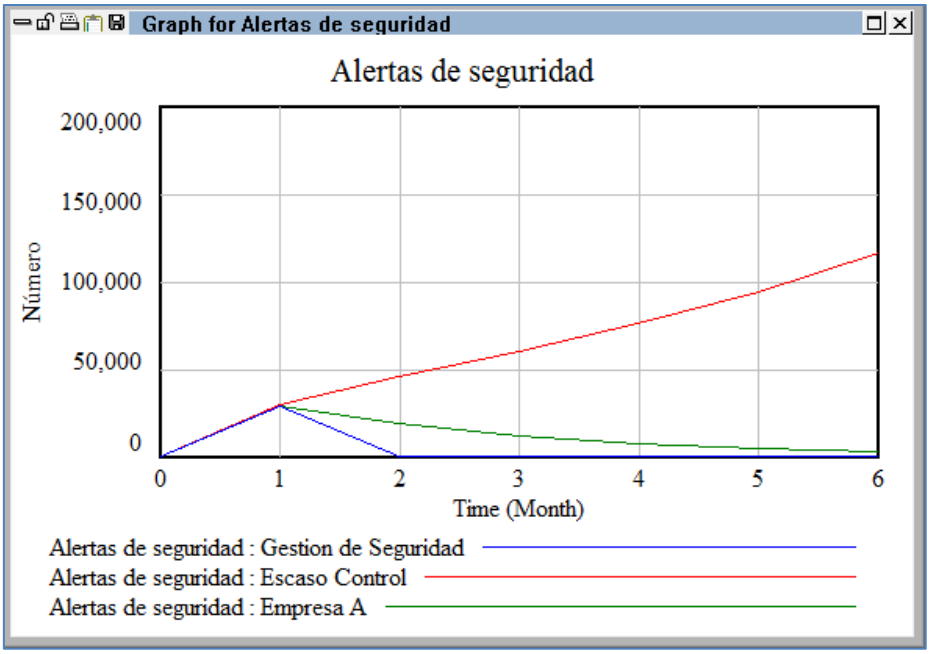


Figura 44. Comparación de las alertas de seguridad en la tercera corrida (Empresa A).

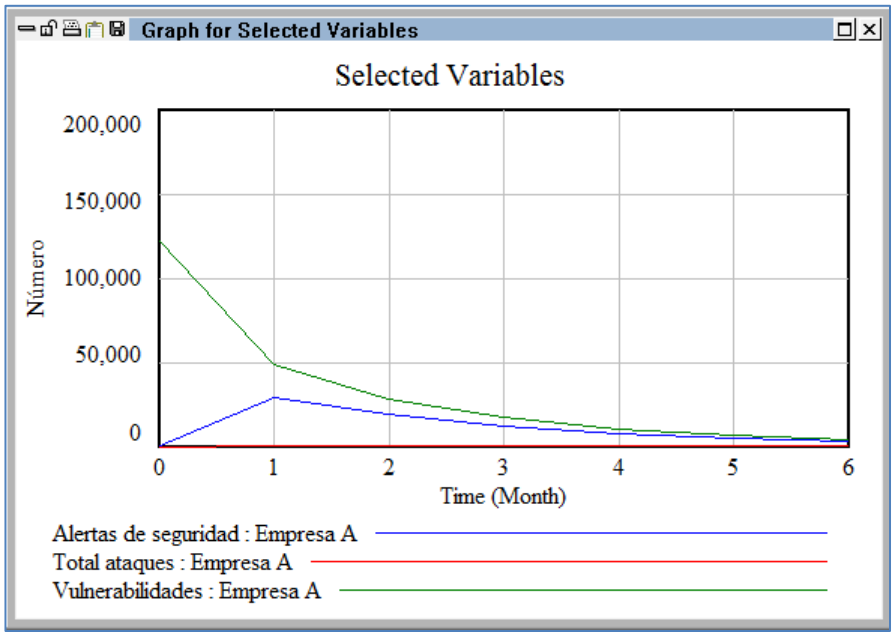


Figura 45. Análisis de las alertas, total de ataques y vulnerabilidades en la tercera corrida (Empresa A).

En la Figura 46 se muestran los valores de alertas, ataques y vulnerabilidades de la Figura 45, resultado de la tercera corrida.

Time (Month)	Selected Variables Runs:	Alertas de seguridad	Total ataques	Vulnerabilidades
	Empresa A			
0		300	0	121618
1		29414.6	151.25	48737.2
2		19201.8	226.875	28364.6
3		11759.2	264.688	17174.5
4		7212.92	283.594	10477
5		4468.95	293.047	6439.74
6		2814.02	297.773	4004.49

Figura 46. Valores en el análisis de las alertas, total de ataques y vulnerabilidades en la tercera corrida. (Empresa A).

En la Figura 47, se observa un escenario estratégico llamado "Empresa AE" en el que la tasa ataques mitigados, tasa de remediación de alertas y el cumplimiento de controles aumentan para el mismo caso de la "Empresa A".

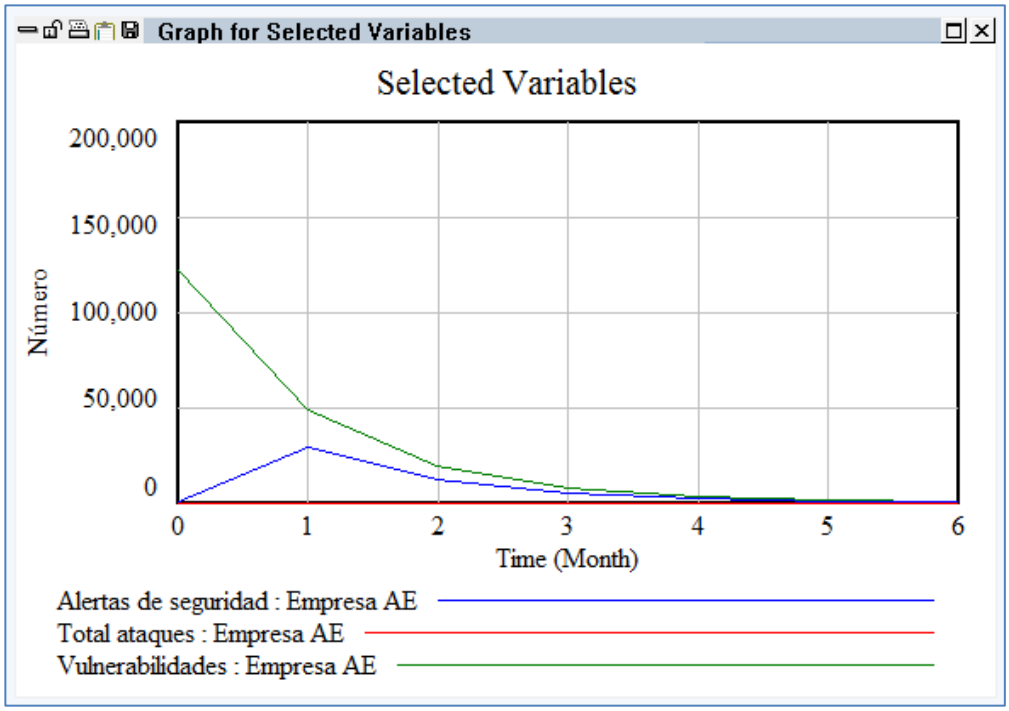


Figura 47. Análisis de las alertas total de ataques y vulnerabilidades en la tercera corrida en un escenario estratégico.

En base a los resultados obtenidos (Figura 47), se evidencia que aplicando la dinámica de sistemas logramos gestionar mejor las vulnerabilidades, puesto que podemos apreciar con mayor visibilidad las causas de tener vulnerabilidades en nuestra organización, en la gráfica se observa una notable disminución de ellas.

Muchas veces se deja pasar los controles, los planes de tratamiento que registra seguridad de la información en el área, un inadecuado seguimiento de los planes de tratamiento son vulnerabilidades que están presentes, también el simple hecho de cumplir con todo no quiere decir que se esté exento de vulnerabilidades, siempre se está propenso a ellas, por ello se analiza el panorama global de las vulnerabilidades y la relación que tienen con los equipos de seguridad.

El modelo ayuda a tomar decisiones estratégicas en seguridad, como en este caso de la Figura 47 se observa que pasaría si la organización mejora su tasa de mitigación de ataque en un 50%, tasa de remediación de alertas en un 25 % y el cumplimiento de controles en un 30%, tendría menos probabilidad a sufrir ataques y aproximadamente a partir del primer mes vería los resultados, es decir menos vulnerabilidades y memos alertas. Por tanto, el modelo nos ayuda a tener una mejor gestión de seguridad.

Las decisiones estratégicas tomadas en este caso de la Figura 47 ayuda a analizar nuestro proceso que tienen una perspectiva reactiva hacia una forma preventiva, se puede considerar la actualización y revisión del software del equipo de seguridad como el switch, revisar si se está cumpliendo con el monitoreo y en qué medida, mejorando así los procesos gestión de la seguridad.

CAPÍTULO 5: RESULTADOS Y CONTRASTACIÓN DE LA HIPÓTESIS

En el presente capítulo se detalla los resultados de la corrida del modelo para un periodo de treinta meses y la validación de la hipótesis establecida inicialmente mediante la t - Student.

5.1 Resultados

En la Tabla 21 se puede observar los diferentes valores que toman los indicadores, la Pre-Prueba está basada sin aplicar el modelo, cuantas alertas, ataques y vulnerabilidades registran por mes, la Post-Prueba es aplicando el modelo.

Se puede identificar que los valores de la Post-Prueba en la corrida del modelo corresponden al intervalo aceptable y en otros casos de cuidado para el indicador, además se ha logrado reducir las alertas, amenazas y vulnerabilidades, por tanto, resulta favorable para el indicador.

Se ha realizado la corrida del modelo en cada uno de los treinta escenarios recopilados de la empresa para la contrastación de la hipótesis.

Tabla 21. Valores de los indicadores en el modelo

Nro	Número de Alertas de Seguridad/mes		Número de ataques/mes		Número de vulnerabilidades/mes	
	Pre-Prueba	Post-Prueba	Pre-Prueba	Post-Prueba	Pre-Prueba	Post-Prueba
1	890	223	165	2	1659	111
2	886	222	161	2	1523	93
3	1372	343	202	3	2010	155
4	1258	315	199	3	1964	150
5	2123	475	270	4	2514	220
6	228	57	36	0	234	29
7	617	154	115	1	908	15
8	500	125	96	0	475	60
9	958	240	178	3	1846	134
10	847	260	126	1	1165	48
11	1245	311	181	3	1921	144
12	2163	497	273	5	2888	267
13	613	153	107	1	864	9
14	2259	474	289	5	2978	279
15	1584	396	206	3	2087	165
16	602	151	106	1	651	82
17	1675	419	230	4	2345	198
18	1901	475	258	4	2350	199
19	955	239	175	2	1758	123
20	225	56	25	0	29	3
21	2107	446	260	4	2467	214
22	2314	474	290	6	2997	199
23	5	1	15	0	7	0
24	593	148	103	1	616	78
25	132	33	16	0	22	2
26	2250	494	285	5	2972	278
27	898	315	167	2	1701	116
28	229	57	79	0	304	38
29	1611	403	217	4	2209	181
30	867	217	158	2	1322	68

5.2 Prueba de normalidad de los datos

5.2.1 I1: Número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.

En la Figura 48 se observa la distribución normal en la Pre-Prueba para el Indicador (I1), y en la Figura 49 en la Post-Prueba para el Indicador (I1), se puede evidenciar que p (0.072, 0.117) > ∝ (0.05). Por lo tanto, los valores del indicador tienen un comportamiento normal.

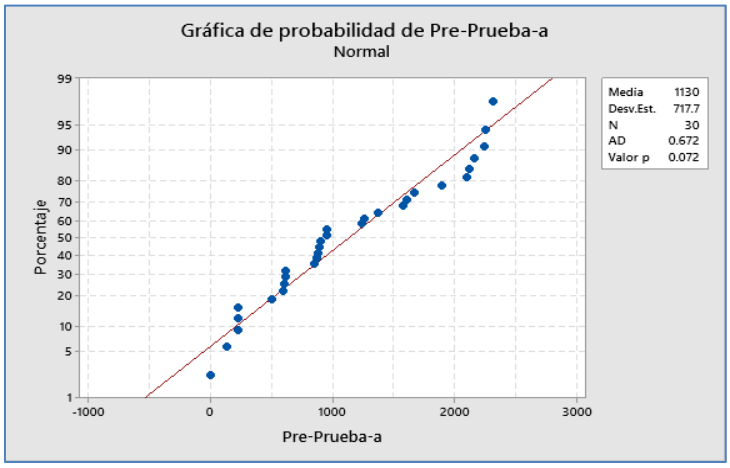


Figura 48. Prueba de Normalidad para el número de alertas (Pre-Prueba).

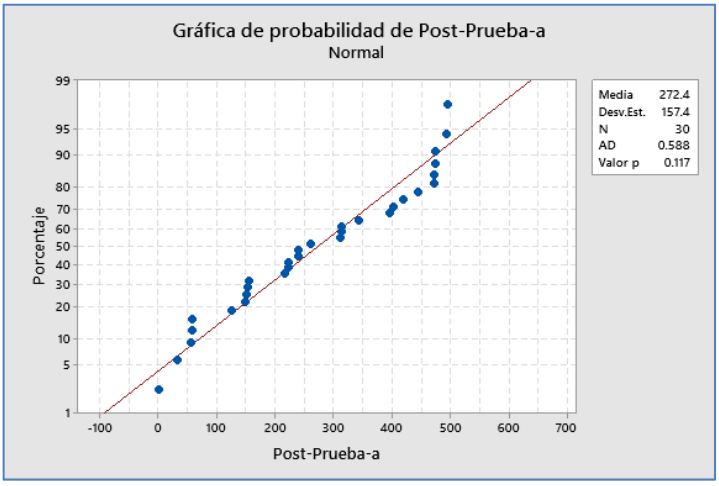


Figura 49. Prueba de Normalidad para el número de alertas (Post-Prueba).

5.2.2 I2: Número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.

En la Figura 50 se observa la distribución normal en la Pre-Prueba para el Indicador (I2) y en la Figura 51 en la Post-Prueba para el Indicador (I2), en ambos casos se puede evidenciar que p (0.417, 0.061) > ∝ (0.05). Por tanto, los valores del indicador tienen un comportamiento normal.

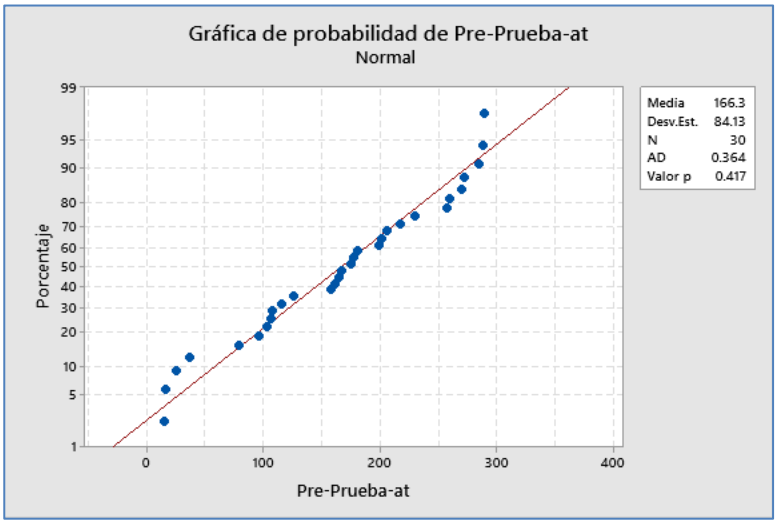


Figura 50. Prueba de Normalidad para el número de ataques (Pre-Prueba).

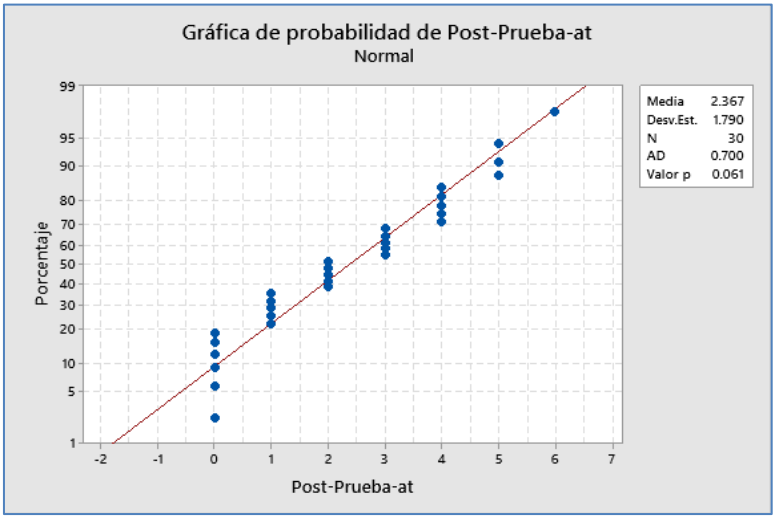


Figura 51. Prueba de Normalidad para el número de ataques (Post-prueba).

5.2.3 I3: Número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.

En la Figura 52 se observa la distribución normal en la Pre-Prueba para el Indicador (I3) y en la Figura 53 la distribución normal en la Post-Prueba para el Indicador (I3), en ambos casos se puede evidenciar que p (0.205, 0.461) > ∝ (0.05). Por tanto, los valores del indicador tienen un comportamiento normal.

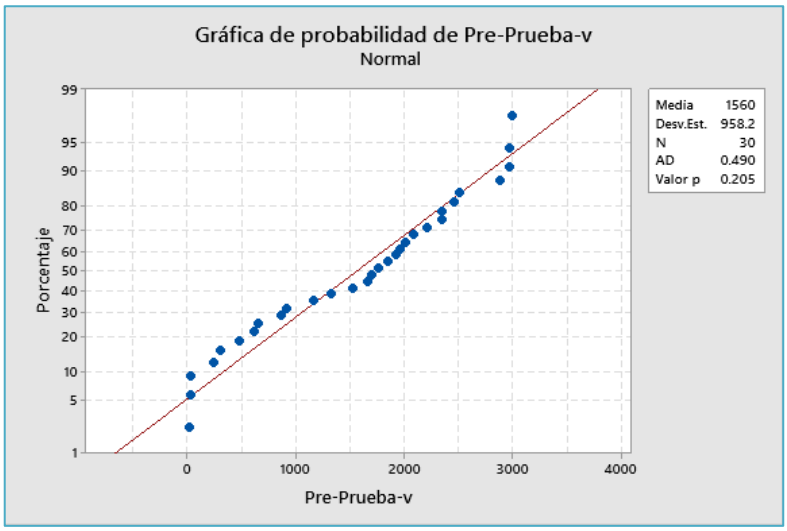


Figura 52. Prueba de Normalidad para el número de vulnerabilidades (Pre - Prueba).

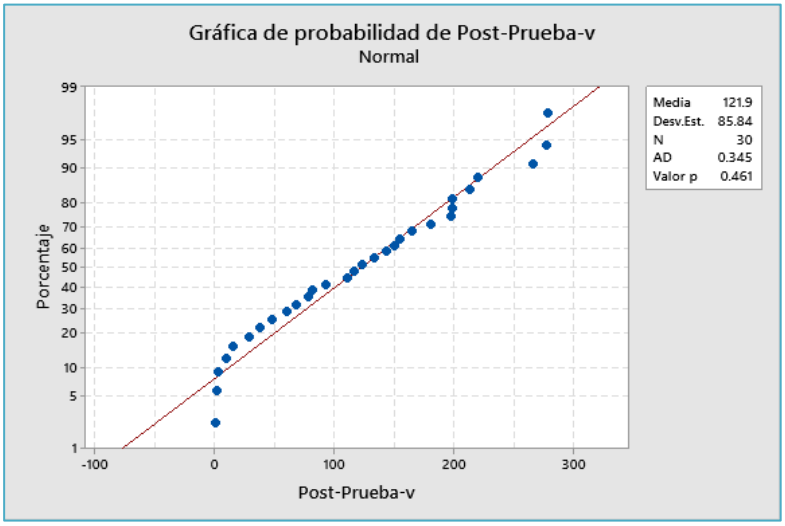


Figura 53. Prueba de Normalidad para el número de vulnerabilidades (Post-Prueba).

5.3 Contrastación de la hipótesis

5.3.1 Contrastación para H1

Si se usa un modelo dinámico, entonces disminuye el número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.

5.3.1.1 Planteamiento de la hipótesis Nula y Alterna:

H0: Si se usa un modelo dinámico, entonces aumenta el número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.

Ha: Si se usa un modelo dinámico, entonces disminuye el número de alertas que influyen en la gestión de seguridad de la infraestructura de las TIC.

μ_1: Media poblacional del número de alertas obtenidas en la Pre-Prueba.

μ_2: Media poblacional del número de alertas obtenidas en la Post-Prueba

$$H0 : \mu_1 \leq \mu_2$$

$$Ha : \mu_1 > \mu_2$$

5.3.1.2 Cálculo: Valor p y Prueba t para medias de las dos muestras

En la Figura 54 se puede observar el cálculo del valor p acorde a los resultados obtenidos antes de la corrida del modelo y con el modelo para número de alertas.

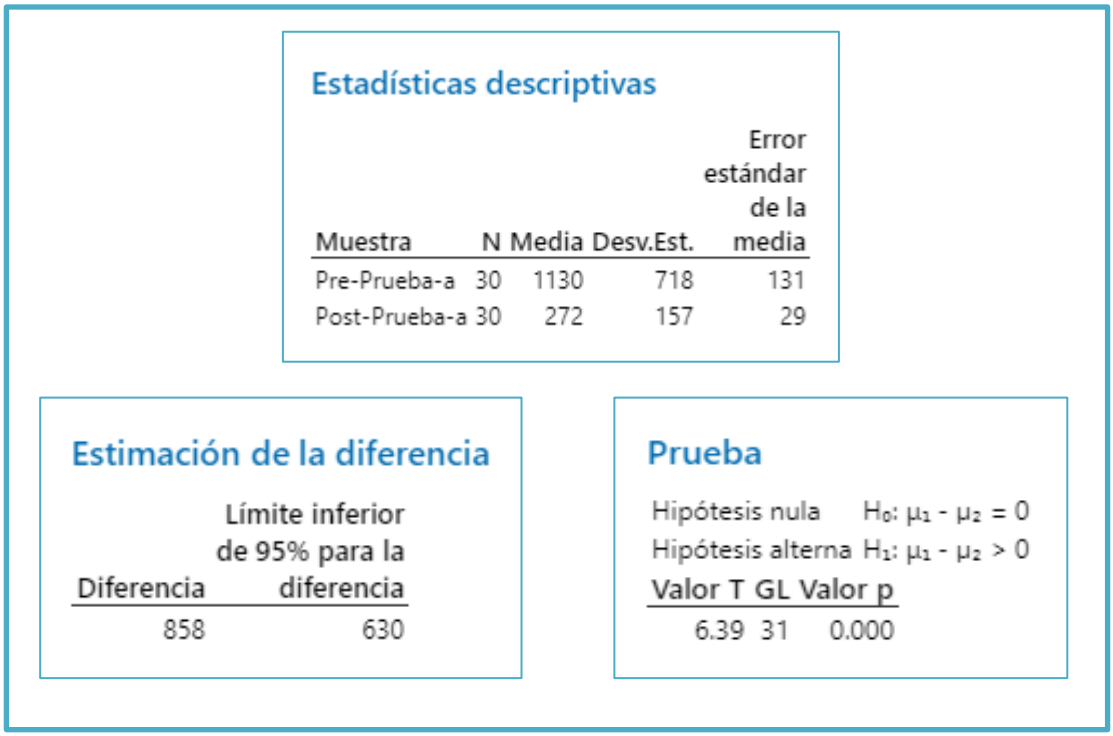


Figura 54. Valor p para el número de alertas

5.3.1.3 Decisión estadística

Puesto que el valor p $(0.000) < \propto (0.05)$, los resultados proporcionan suficiente evidencia para rechazar la hipótesis nula (H0) y la hipótesis alterna (Ha) es cierta. La prueba resultó ser significativa.

5.3.2 Contrastación para H2

Si se usa un modelo dinámico, entonces disminuye el número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.

5.3.2.1 Planteamiento de la hipótesis Nula y Alterna:

H0: Si se usa un modelo dinámico, entonces aumenta el número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.

Ha: Si se usa un modelo dinámico, entonces disminuye el número de ataques que influyen en la gestión de seguridad de la infraestructura de las TIC.

μ_1: Media poblacional del número de ataques obtenidas en la Pre-Prueba.

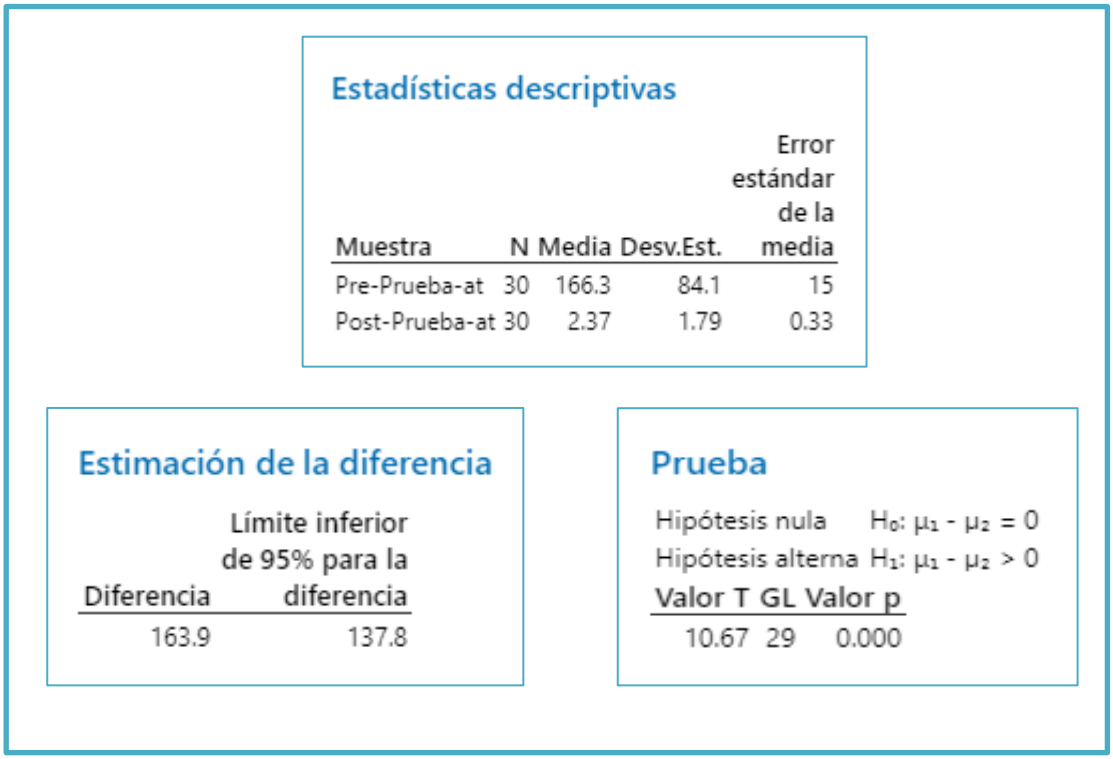
μ_2: Media poblacional del número de ataques obtenidas en la Post-Prueba

$$H0 : \mu_1 \leq \mu_2$$

$$Ha : \mu_1 > \mu_2$$

5.3.2.2 Cálculo: Valor p y Prueba t para medias de las dos muestras

En la Figura 55 se puede observar el cálculo del valor p acorde a los resultados obtenidos antes de la corrida del modelo y con el modelo para número de ataques.



Estadísticas descriptivas

Muestra	N	Media	Desv.Est.	Error estándar de la media
Pre-Prueba-at	30	166.3	84.1	15
Post-Prueba-at	30	2.37	1.79	0.33

Estimación de la diferencia

Diferencia	Límite inferior de 95% para la diferencia
163.9	137.8

Prueba

Hipótesis nula $H_0: \mu_1 - \mu_2 = 0$

Hipótesis alterna $H_1: \mu_1 - \mu_2 > 0$

Valor T	GL	Valor p
10.67	29	0.000

Figura 55. Valor p para el número de ataques

5.3.2.3 Decisión estadística

Puesto que el valor p (0.000) $< \propto (0.05)$, los resultados proporcionan suficiente evidencia para rechazar la hipótesis nula (H0) y la hipótesis alterna (Ha) es cierta. La prueba resultó ser significativa.

5.3.3 Contrastación para H3

Si se usa un modelo dinámico, entonces disminuye el número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.

5.3.3.1 Planteamiento de la hipótesis Nula y Alterna:

H0: Si se usa un modelo dinámico, entonces aumenta el número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.

Ha: Si se usa un modelo dinámico, entonces disminuye el número de vulnerabilidades que influyen en la gestión de seguridad de la infraestructura de las TIC.

μ_1: Media poblacional del número de vulnerabilidades obtenidas en la Pre-Prueba.

μ_2: Media poblacional del número de vulnerabilidades obtenidas en la Post-Prueba

$$\text{H0} : \mu_1 \leq \mu_2$$

$$\text{Ha} : \mu_1 > \mu_2$$

5.3.3.2 Cálculo: Valor p y Prueba t para medias de las dos muestras

En la Figura 56 se puede observar el cálculo del valor p acorde a los resultados obtenidos antes de la corrida del modelo y con el modelo para número de vulnerabilidades.

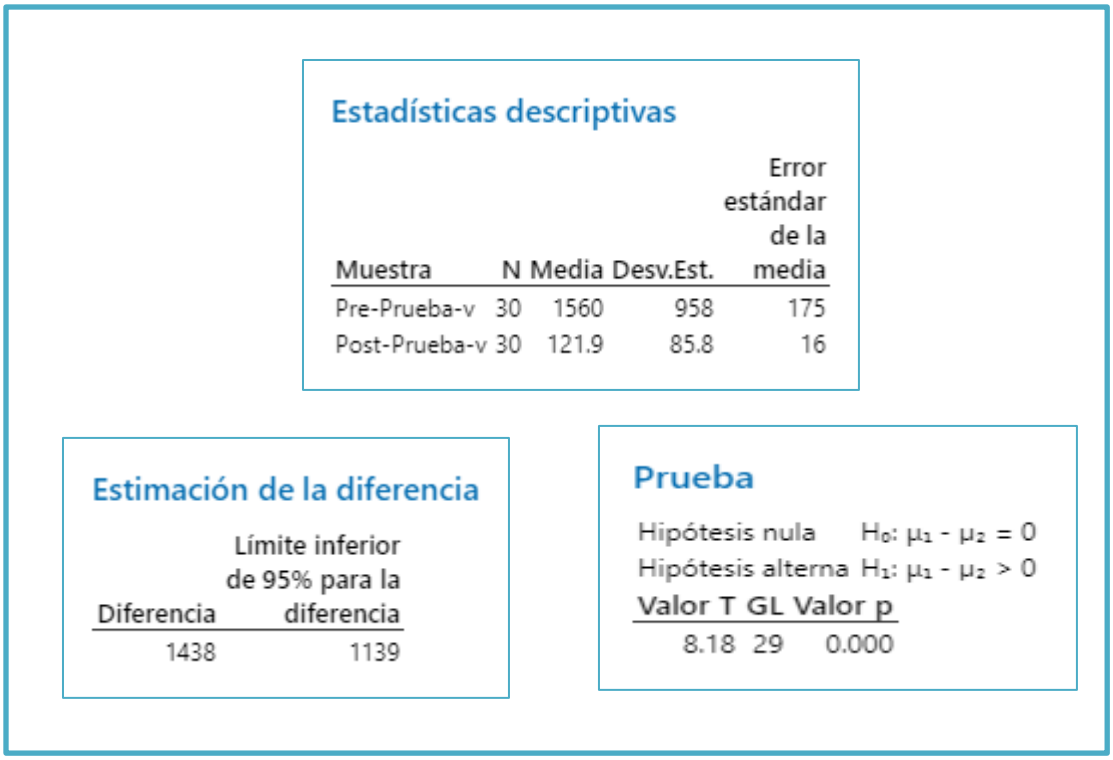


Figura 56. Valor p para el número de vulnerabilidades.

5.3.3.3 Decisión estadística

Puesto que el valor p $(0.000) < \propto (0.05)$, los resultados proporcionan suficiente evidencia para rechazar la hipótesis nula (H0) y la hipótesis alterna (Ha) es cierta. La prueba resultó ser significativa.

CAPÍTULO 6: CONCLUSIONES Y TRABAJOS FUTUROS

6.1 Conclusiones

a) Se demostró que el uso del modelo ayuda a tomar mejores decisiones para los encargados de seguridad, logrando la disminución del número de alertas que reportan las diferentes áreas.

b) Al evaluar los diferentes escenarios se evidenció que el uso del presente modelo favorece con una respuesta inmediata ante los posibles ataques. Además, se logra su prevención.

c) Se comprobó a través de las corridas y con decisiones estratégicas que la aplicación del modelo basado en la dinámica de sistemas contribuyó a minimizar el número de vulnerabilidades.

6.2 Trabajos Futuros

a) Se puede incluir otros aspectos como las características de los equipos, que complementen la idea global de la seguridad informática, puesto que resulta muy amplio abarcar todo.

b) La presente tesis puede ser aplicada en diferentes dominios de la ISO 27001.

c) Se puede construir una aplicación basada en el modelo que a partir de la data ingresada muestre los resultados de forma más interactiva para los encargados de seguridad.

d) Se puede incluir técnicas de inteligencia artificial en el modelo, para construir otras herramientas que capturen de forma automática valores de vulnerabilidades y ataques reportados en el mundo por diversas entidades; entonces, ya no se necesitaría estar actualizado el modelo, si no que automáticamente cambiaría de acuerdo con la información generada.

Referencias Bibliográficas

Tesis

Pastor, C. (2010). *Impacto del Riesgo en el Gobierno de las Tecnologías de Información y Comunicación en la Gestión Empresarial del Siglo XXI. Para obtener el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con Mención en Dirección y Gestión de Tecnologías de información. Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas e Informática. Lima, Perú.*

Mendoza, M. (2018). *Modelo de dinámica de sistemas para la evaluación de estrategias de fidelización al cliente. Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con Mención en Gestión de Tecnologías de la Información, Universidad Nacional Federico Villareal. Lima, Perú. Recuperado el 01 de Enero de 2020, de http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2857/MENDOZA%20DIONICIO%20MIGUEL%20ABDIAS%20-%20MAESTRIA.pdf?sequence=1&isAllowed=y*

Artículos- Informes-Páginas Web

Aracil, J. (1997). *Dinámica de sistemas.* Alianza Universidad textos.

Bela, G., Kiss, I., & Piroska, H. (2015). *A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures.* International Journal of Critical Infrastructure Protection. doi:10.1016/j.ijcip.2015.04.001

Boiko, A., & Shendryk, V. (2017). *System Integration and Security of Information Systems.* doi:10.1016/j.procs.2017.01.053

Cisco. (2016). *Informe anual sobre ciberseguridad.* Recuperado el 27 de Mayo de 2018, de https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

Cisco. (2017). *Informe anual sobre ciberseguridad.* Recuperado el 27 de Mayo de 2018, de https://www.cisco.com/c/dam/m/digital/1226019/Cisco_2017_ACR_es-xl.pdf

Cisco. (2017). *Reporte Semestral de Seguridad.* Recuperado el 27 de Mayo de 2018, de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cisco-reporte-semestral-2017-espanol.pdf

CONCYTEC. (2016). *Programa Nacional Transversal de Tecnologías de la Información y Comunicación 2016 -2021. 1a edición.* Depósito Legal en la Biblioteca Nacional del Perú Nº 2016-09849. Recuperado el 10 de Mayo de 2018, de https://portal.concytec.gob.pe/images/publicaciones/libro_tics_oct.pdf

D.L. Nazareth, J. C. (2015). A System Dynamics Model for Information Security management, Information and Management. En *Information & Management* (págs. 123-134).

ENISA. (2017). *Threat Landscape Report 2016 15 Top Cyber-Threats and Trends.* Recuperado el 15 de Mayo de 2017, de Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Fagade, T., Spyridopoulos, T., Albishry, N., & Tryfonas, T. (2017). *System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis.* Springer International Publishing. Cham: Tryfonas T.

Gendron, M. (2012). *Business Intelligence Applied: Implementing an Effective Information and Communications Technology Infrastructure.* John Wiley & Sons.

GhasemiGol, M., Takabi, H., & Ghaemi-Bafghi, A. (2016). *A foresight model for intrusion response management.* doi:10.1016/j.cose.2016.06.005

Guckenheimer, J., & Ellner, S. (2011). Dynamic Models in Biology. En J. Guckenheimer, & S. Ellner. Princeton University Press.

Huawei. (28 de Diciembre de 2018). *HiSec: Intelligent active defense for ICT infrastructure*. (D. Song, Productor, & Huawei Network Security Domain) Recuperado el 8 de Octubre de 2019, de https://www.huawei.com/fr/about-huawei/publications/communicate/86/hisec-intelligent-active-defense

Huawei Technologies Co. (2018). *TELCO: INVESTMENT, INNOVATION.* Recuperado el 10 de Octubre de 2019, de https://www-file.huawei.com/-/media/corporate/pdf/public-policy/huawei_ict_position_paper_v2.pdf?la=en

IBM. (2018). *IBM X-Force Threat Intelligence Index 2018.* Recuperado el 02 de Junio de 2018, de https://securityintelligence.com/

Incibe. (2017). *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.* Ministerio de Energía, Turismo y Agenda Digital, España. Recuperado el 19 de Octubre de 2019, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

ISACA. (2010). *The Business Model for Information Security.* United States of America.

ISACA. (2012). *COBIT 5 for Information Securit.* United States of America: ISACA. Recuperado el 10 de 10 de 2019, de https://m.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

ISACA. (2013). *Process Assessment Model (PAM): Using COBIT® 5.*

ISACA. (2015). *Global Cybersecurity Status Report.* Recuperado el 30 de Mayo de 2017, de https://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf

ISACA. (2015). *Glossary of Terms – Spanish 3rd Edition.* Recuperado el 12 de Agosto de 2019, de https://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Spanish_mis_Spa_0615.pdf

ISACA. (2016). *State of Cybersecurity.* Recuperado el 15 de Mayo de 2017, de https://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2016.aspx

ISACA, Protiviti. (2017). *A Global Look at IT Audit Best Practices.* Recuperado el 10 de Octubre de 2019, de http://www.isaca.org/Knowledge-Center/Research/Documents/6th-Annual-IT-Audit-Benchmarking-Survey-ISACA-Protiviti-mis_eng_0217.pdf

ISACA, Protiviti. (2019). *Today's Toughest Challenges in IT.* Recuperado el 09 de Septiembre de 2019, de http://www.isaca.org/Knowledge-Center/Research/Documents/2019-Global-IT-Audit-Benchmarking-Study-Exec-Summary_res_eng_0519.PDF?regnum=

ISO/IEC 27000. (2009). *Information technology — Security techniques — Information security management systems.* Recuperado el 10 de Octubre de 2019, de https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27000:ed-1:v1:en

Khalil. (2016). *A Novel Probabilistically-Timed Dynamic Model for Physical Security Attack Scenarios on Critical Infrastructures.* Physical Sciences Department, United Technologies Research Center (UTRC). doi:10.1016/j.psep.2016.05.001

Kondakci, S. (2015). *Analysis of information security reliability: A tutorial*. doi:10.1016/j.ress.2014.09.021

Mai, B., Parsons, T., Prybutok, V., & Namuduri, K. (2017). *Information Systemas and Neuroscience "Neurosciencie Foundations for Human Decision Making in Information Security"*. Springer. doi:10.1007/978-3-319-41402-7_12

Massachusetts Institute of Technology. (1997). *The First Step.* Recuperado el 15 de 02 de 2020, de https://ocw.mit.edu/courses/sloan-school-of-management/15-988-system-dynamics-self-study-fall-1998-spring-1999/readings/step.pdf

Mathew, S., & Pauline, A. (2016). *HTTP Botnet Defense Mechanism using System Dynamics based Genetic Algorithm.* Indian Journal of Science and Technology. doi:10.17485/ijst/2016/v9i45/106506

Matthew, I., & Zheng, W. (1 de Agosto de 2017). *Modelado de sistemas dinámicos*. doi:10.1002/9781118901731.iecrm0074

Meerschaert, M. (2013). Introduction to Dynamic Models. *Mathematical Modeling*, 115-137. doi:10.1016/B978-0-12-386912-8.50004-X

Miyamoto, I., Holzer, T., & Sarkani, S. (2017). *Why a counterfeit risk avoidance strategy fails.* doi:10.1016/j.cose.2016.12.015

Moore, A., Carley, K., Collins, M., & Altman, N. (2015). *Social network dynamics of insider threats: a preliminary model.* Obtenido de https://www.researchgate.net/publication/303868482_Social_Network_Dynamics_of_Insider_Threats_A_Preliminary_Model

NIST. (2016). *NIST Special Publication 800-150- Guide to Cyber Threat Information Sharing.* doi:10.6028/NIST.SP.800-150

NTP-ISO/IEC 27001. (2014). *TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de la seguridad de la infomación. Requisitos.*

Okoye, S. I. (2017). *Strategies to minimize the effects of information security threats on business performance (Order No. 10606454).* Walden University. Obtenido de https://search.proquest.com/docview/1944007406?accountid=161077

Parada, D., Flórez, A., & Gómez, U. (2018). *Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas.* doi:10.4067/S0718-07642018000100027

Roumani, M., Fung, C. C., & Choejey, P. (2015). *Assessing economic impact due to cyber attacks with System Dynamics approach.* 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Hua Hin. doi:10.1109/ECTICon.2015.7207084

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2016). *A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM).* International Conference on Information Systems and Computer Science (INCISCOS). doi:10.1109/INCISCOS.2017.20

Senge, P. M. (2006). *La Quinta Disciplina en la Práctica. Estrategias y herramientas para construir la organización abierta al aprendizaje* (Primera ed.). GRANICA.

Senge, P. M. (2010). *La Quinta Disciplina. El arte y la práctica de la organización abierta al aprendizaje* (Segunda ed.). GRANICA.

Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. (2015). *A secure control framework for resource-limited adversaries.* doi:10.1016/j.automatica.2014.10.067

Tonhauser, M., & Ristvej, J. (2019). *Disruptive acts in cyberspace, steps to improve cyber resilience at National Level.* doi:10.1016/j.trpro.2019.07.220

Wang, R., Rho, S., Chen, B., & Cai, W. (2017). *Modeling of large-scale social network services based on mechanisms of information diffusion: Sina Weibo as a case study.* doi:10.1016/j.future.2016.03.018

WEF. (2018). *To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity.* Recuperado el 27 de Mayo de 2018, de https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/

WEF. (2019). *The Global Risks Report 2019 14 th Edition.* Recuperado el 12 de Octubre de 2019, de http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf